This is a digital copy of a book that was preserved for generations on library shelves before it was carefully scanned by Google as part of a project to make the world's books discoverable online.

It has survived long enough for the copyright to expire and the book to enter the public domain. A public domain book is one that was never subject to copyright or whose legal copyright term has expired. Whether a book is in the public domain may vary country to country. Public domain books are our gateways to the past, representing a wealth of history, culture and knowledge that's often difficult to discover.

Marks, notations and other marginalia present in the original volume will appear in this file - a reminder of this book's long journey from the publisher to a library and finally to you.

Usage guidelines

Google is proud to partner with libraries to digitize public domain materials and make them widely accessible. Public domain books belong to the public and we are merely their custodians. Nevertheless, this work is expensive, so in order to keep providing this resource, we have taken steps to prevent abuse by commercial parties, including placing technical restrictions on automated querying.

We also ask that you:

+ *Make non-commercial use of the files* We designed Google Book Search for use by individuals, and we request that you use these files for personal, non-commercial purposes.

+ *Refrain from automated querying* Do not send automated queries of any sort to Google's system: If you are conducting research on machine translation, optical character recognition or other areas where access to a large amount of text is helpful, please contact us. We encourage the use of public domain materials for these purposes and may be able to help.

+ *Maintain attribution* The Google "watermark" you see on each file is essential for informing people about this project and helping them find additional materials through Google Book Search. Please do not remove it.

+ *Keep it legal* Whatever your use, remember that you are responsible for ensuring that what you are doing is legal. Do not assume that just because we believe a book is in the public domain for users in the United States, that the work is also in the public domain for users in other countries. Whether a book is still in copyright varies from country to country, and we can't offer guidance on whether any specific use of any specific book is allowed. Please do not assume that a book's appearance in Google Book Search means it can be used in any manner anywhere in the world. Copyright infringement liability can be quite severe.

About Google Book Search

Google's mission is to organize the world's information and to make it universally accessible and useful. Google Book Search helps readers discover the world's books while helping authors and publishers reach new audiences. You can search through the full text of this book on the web at `http://books.google.com/`

Math 2319.03.5

Harvard College Library

FROM

The University

SCIENCE CENTER LIBRARY

THE UNIVERSITY OF CHICAGO
FOUNDED BY JOHN D. ROCKEFELLER

THE DECENNIAL PUBLICATIONS

SUBGROUPS OF THE GENERALIZED FINITE MODULAR GROUP

BY
HOMER HASTINGS HOUSE

The Decennial Publications

First Series

Two volumes of thirteen and eight volumes of Investigations, the latter consisting of a collection of articles representing the work of research of the several departments of the University. Size, quarto.

Volume I. The President's Report. A Administration.

Volume II. The President's Report. B Publications of the Members of the University.

Volume III. Part 1. — Systematic Theology, Church History, Comparative Theology.

Part 2. — Philosophy, Education.

Volume IV. Political Economy, Political Science, History, Sociology.

Volume V. Semitic Languages and Literatures, Biblical and Patristic Greek, Comparative Religion.

Volume VI. Greek Language and Literature, Latin Language and Literature, Sanskrit and Indo-European Comparative Philology, Classical Archæology.

Volume VII. Romance Languages and Literatures, Germanic Languages and Literatures, English, Literature in English.

Volume VIII. Astronomy and Astrophysics.

Volume IX. Mathematics, Physics, Chemistry, Geology.

Volume X. Zoology, Anatomy, Physiology, Neurology, Botany, Pathology, Bacteriology.

Second Series

A series of volumes embodying original research, consisting of systematic treatises, annotated documents, and the like. Size, octavo.

THE UNIVERSITY OF CHICAGO
FOUNDED BY JOHN D. ROCKEFELLER

THE DECENNIAL PUBLICATIONS

THE SUBGROUPS OF THE GENERALIZED FINITE MODULAR GROUP

BY

ELIAKIM HASTINGS MOORE

PROFESSOR AND HEAD OF THE DEPARTMENT OF MATHEMATICS

PRINTED FROM VOLUME IX

CHICAGO
THE UNIVERSITY OF CHICAGO PRESS
1903

Prot. 231.03.5

The University

Copyright 1903
BY THE UNIVERSITY OF CHICAGO

THE SUBGROUPS OF THE GENERALIZED FINITE MODULAR GROUP

ELIAKIM HASTINGS MOORE

INTRODUCTION

THE modular group Γ of all unimodular substitutions $(\alpha, \beta; \gamma, \delta)$

$$\omega' = \frac{\alpha\omega + \beta}{\gamma\omega + \delta} \qquad (\alpha\delta - \beta\gamma = 1)$$

of the complex variable ω, where the α, β, γ, δ are rational integers, has for every rational prime q a self-conjugate subgroup $\Gamma_{\mu(q)}$ of finite index $\mu(q)$ containing all substitutions $(\alpha, \beta; \gamma, \delta)$ for which $\alpha \equiv 1, \beta \equiv 0, \gamma \equiv 0, \delta \equiv 1 \pmod{q}$. The corresponding quotient-group $\Gamma/\Gamma_{\mu(q)}$ is conveniently given as the say finite modular group $G^{q+1}_{\mu(q)}$ of substitutions $(\alpha, \beta; \gamma, \delta)$ on the $q+1$ marks ω ($\omega = \infty, 0, 1, \cdots, q-1$) where the α, β, γ, δ are integers taken modulo q. (*Cf.* Klein-Fricke, *Theorie der elliptischen Modulfunctionen*, Vol. I, pp. 419–91.) By generalizing from the Galois-field of rank 1 to that of rank n ($GF[q^n]$; Galois's imaginaries) we have the generalized finite modular group $G^{q^n+1}_{M(q^n)}$ of order $M(q^n) = q^n(q^{2n}-1)$ or $q^n(q^{2n}-1)/2$ according as $q = 2$ or $q > 2$. Mathieu first exhibited this group and studied its cyclic subgroups (*Comptes rendus*, 1858, 1859; *Liouville's Journal*, 1860, p. 39). That (except for the cases $q^n = 2^1$, 3^1) it is simple was proved by myself (*Mathematical Papers of the Chicago Congress*, 1893, pp. 208–42; published in 1896; in abstract, *Bulletin of the New York Mathematical Society*, December, 1893, Vol. III, pp. 73–8), and independently, but incompletety, by Burnside (*Proceedings of the London Mathematical Society*, Vol. XXV, pp. 113–39, February, 1894).

In the present paper all subgroups of the $G^{q^n+1}_{M(q^n)}$ are determined; for the case $n = 1$ this was done by Gierster (*Mathematische Annalen*, Vol. XVIII (1881)). The subgroups are of three kinds: (1) metacyclic or solvable groups; (2) (3) groups of the abstract character of certain groups $G^{q^n+1}_{M(q^n)}$ or of certain groups $G^{q^n+1}_{\frac{1}{2}M(q^n)}$ ($q > 2$), a group $G^{q^n+1}_{\frac{1}{2}M(q^n)}$ being obtained by extending the $G^{q^n+1}_{M(q^n)}$ by the substitution $\omega' = \rho\omega$, where ρ is a primitive root of the $GF[q^n]$. Thus the doubly infinite system of simple groups

$$G^{q^n+1}_{M(q^n)} \qquad (q \neq 2^1, 3^1)$$

determines by the decomposition of the subgroups of its constituent groups, apart from the simple groups of prime order, only simple groups of the original system. An equation of degree $q^n + 1$ ($q^n \neq 2^1, 3^1$) whose Galois-group is the $G^{q^n+1}_{M(q^n)}$ has resolvents

of degree D, $D < q^n + 1$, only in the cases $q^n = 5^1, 7^1, 11^1, 3^2$, when D is respectively 5, 7, 11, 6. For $n = 1$ this is a noted theorem of Galois and Gierster.

The group $\Gamma[\Omega]$ of all unimodular substitutions $(\alpha, \beta; \gamma, \delta)$ where the coefficients are algebraic integers of an algebraic field Ω [Körper Ω] has for every prime functional π [Weber] of absolute norm q^n, a self-conjugate subgroup $\Gamma_{M(q^n)}[\Omega]$. The quotient-group is the group $G^{q^n+1}_{M(q^n)}$. The substitutions of the modular group Γ leave invariant a modular function $J(\omega)$. The transcendental modular equation $J = J(\omega)$ has algebraic resolvents, modular equations, with Galois-groups $G^{q+1}_{M(q)=\mu(q)}$. The group $\Gamma[\Omega]$, for field Ω of degree > 1, is improperly discontinuous and has no corresponding automorphic function. If however an automorphic function $K(\omega)$ belongs to a group whose substitutions have coefficients of an algebraic field Ω, then the generalized modular equation $K = K(\omega)$ has algebraic resolvents whose Galois-groups are certain generalized finite modular groups $G^{q^n+1}_{M(q^n)}$ or certain of their subgroups. This remark connects the present paper with the recent work of Fricke and Bianchi on certain special classes of automorphic functions (*cf.* Fricke-Klein, *Automorphe Functionen*, Vol. I (1897), pp. 585 ff.).

This paper was read before the American Mathematical Society at the Boston meeting, August, 1898. The preceding paragraphs are, with insignificant modifications, the abstract of the paper incorporated (pp. 7, 8) in the report of the secretary of the society as published in the *Bulletin* of the society for October, 1898 (Vol. V, No. 1). The paper was to be offered to the *Mathematische Annalen*. Wishing, however, to develop the ideas of the last paragraph of the abstract, I held the paper back. The following year, April 12, 1899, Wiman presented to the Swedish Academy his memoir: *Bestimmung aller Untergruppen einer doppelt unendlichen Reihe von einfachen Gruppen* (*Bihang till K. Svenska Vet.-Akad. Handlingar*, Vol. XXV, Part I, No. 2).

Only slightly modified from its form of August, 1898, I am now publishing my paper. I enter into no comparison with the treatments of Burnside (*loc. cit.*) for $q = 2$, of Wiman and of Dickson (*Linear Groups*, Teubner, 1901, §§ 68–71, 239–63, based on my MS. and the memoir of Wiman).

In § 1 the theorems of generational determination of the symmetric and the alternating groups are stated. In §§ 2, 3, the properties of the finite field (endliche Körper), in particular that every finite field is the abstract form of a Galois-field, are developed. §§ 4, 5 are devoted to the definitions of the "real" and two "imaginary" forms of the group under consideration, while in § 6 the individual operators and the "largest" cyclic and commutative subgroups of the $G_{M(s)}$ $(s = q^n)$ are determined and classified as to conjugacy. §§ 2–6 come for the most part without change from my Chicago Congress paper of 1893, and form an integral part of this paper. In § 8 is proved the simplicity of the $G_{M(s)}$ $(s \neq 2^1, 3^1)$; in 1893 I proved this theorem by the elaborate consideration of a single complicated diophantine equation; in the present

proof two of three cases are treated by the use of theorems stated by Burnside and proved in § 3, 51°, and § 7, and the third case is treated by a simple diophantine equation. Of course, the complete enumeration of the subgroups determines this question of simplicity; but a more direct proof is clearly desirable.

In the complete enumeration the new "second imaginary" form $G^{\prime\prime}{}^{s^1+1}_{M(s)}$ (§ 5 (15)) of the $G_{M(s)}$ proves to be serviceable. The study in § 10 of the conjugacy of the commutative subgroups of order a power of q reduces to the study of the multiplier Galois-fields of the additive groups of the basal Galois-field of order q^n, and in this connection in § 11 we meet interesting relations of cyclotomic functions.

The theorem of § 17, generalizing the theorem of Galois and Gierster, as to the exceptional cases $s = q^n = 5^1, 7^1, 11^1, 3^2$, I communicated to Mr. Fricke in a letter dated February 17, 1894.

§ 1. THE ABSTRACT SYMMETRIC AND ALTERNATING GROUPS

(1°) We have the important twofold:

Theorem I.[1]—*If the generators* $\left\{\begin{matrix} B_0, \cdots, B_{k-2} \\ E_1, \cdots, E_{k-2} \end{matrix}\right\}$ *of a group* $\left\{\begin{matrix} G\{B_0, \cdots, B_{k-2}\} \\ G\{E_1, \cdots, E_{k-2}\} \end{matrix}\right\}$ *of order greater than* $\left\{\begin{matrix} 2;\ 6 \\ 1;\ 3 \end{matrix}\right\}$ *for* $\left\{\begin{matrix} k \neq 4;\ k = 4 \\ k \neq 4;\ k = 4 \end{matrix}\right\}$ *satisfy the equations*

$$\left\{\begin{matrix} I = B_d^2 = (B_d B_{d+1})^3 = (B_d B_e)^2 & \left(\begin{matrix} d, d+1, e = 0, 1, \cdots, k-2 \\ e > d+1 \end{matrix}\right) \\ I = E_1^3 = E_{d'}^2 = (E_d E_{d+1})^3 = (E_d E_e)^2 & \left(\begin{matrix} d', d, d+1, e = 1, 2, \cdots, k-2 \\ d' > 1, e > d+1 \end{matrix}\right) \end{matrix}\right. \quad \begin{matrix} (1) \\ (2) \end{matrix},$$

then the group G is of order $\left\{\begin{matrix} k! \\ \frac{1}{2}k! \end{matrix}\right\}$ *and is holoedrically isomorphic with the* $\left\{\begin{matrix} \textit{symmetric} \\ \textit{alternating} \end{matrix}\right\}$ *group on k letters, and the generators satisfy no further independent relations.*

In the substitution-groups on the k letters $l_1, \cdots, l_k$ the generators B_d, E_d are, for instance,

$$B_d = (l_{d+1} l_{d+2}), \quad E_d = B_0 B_d = (l_1 l_2)(l_{d+1} l_{d+2}) \qquad (d, d+1 = 2, 3, \cdots, k). \quad (3)$$

We denote the abstract symmetric and alternating groups by the notations $G^{(k)}_{k!}$, $G^{(k)}_{\frac{1}{2}k!}$.

(2°) *Theorem II.—An abstract group G of elements . . . P . . . having the schematic multiplication table*

$$P_3 = P_1 P_2,$$

the transposed multiplication table

$$Q_3 = Q_2 Q_1$$

in the elements . . . Q . . . in 1 − 1 notational correspondence with the elements . . . P . . . defines an abstract group $\breve{G}$*—the transpose group of the original group.*

[1] MOORE, "Concerning the Abstract Groups of Order $k!$ and $\frac{1}{2}k!$ Holohedrically Isomorphic with the Symmetric and Alternating Substitution-Groups on k Letters," *Proceedings of the London Mathematical Society*, December 10, 1896, Vol. XXVIII (1897), pp. 357-66; Theorems A, B, and C.

A group G identical with its transpose $\breve{G}$ is called a self-transpose group.

(3°) *Theorem III.—The abstract symmetric and alternating groups* $G_{k!}^{(k)}$, $G_{\frac{1}{2}k!}^{(k)}$ *are self-transpose groups.*—To prove for the $G_{\frac{1}{2}k!}^{(k)}$ with elements P and generators E: The group $G_{\frac{1}{2}k!}^{(k)}\{E_1, \cdots, E_{k-2}\}$ is holoedrically transformed into itself $G_{\frac{1}{2}k!}^{(k)}\{F_1, \cdots, F_{k-2}\}$, where $F_d = E_d^{-1}$ $(d = 1, \cdots, k-2)$, since the F_d satisfy the relations (2) of the E_d. But in view of the formula $(P_1P_2)^{-1} = P_2^{-1}P_2^{-1}$ the two groups with elements $\ldots P \ldots$, $\ldots Q \ldots$, where $Q = P^{-1}$ are seen to be transposes each of the other.

(4°) In the substitution-group $G_{M(q)}^{q+1}$ of this paper (§ 4) it is, owing to the analytic form of the substitutions, convenient to denote the substitution compounded from two substitutions, first S, then T, by TS instead of, as usual, by ST.—In view of Theorem III this notational variation will cause no complication in the application of Theorem I.

(5°) *Examples* of concrete forms of the symmetric and alternating groups—in the notations[2] of § 4.

SYMMETRIC GROUPS $G_{k!}$

	k	$k!$	Group	B_0	B_1	B_2	B_3	B_4
(I)	3	6	$G_{M(2)}^{3}$	$\left(\frac{1, 1}{0, 1}\right)$	$\left(\frac{1, 0}{1, 1}\right)$			
(II)	4	24	$G_{\frac{1}{2}M(3)}^{4}$	$\left(\frac{-1, 0}{0, 1}\right)$	$\left(\frac{-1, -1}{0, 1}\right)$	$\left(\frac{0, 1}{1, 0}\right)$		
(III)	5	120	$G_{\frac{1}{2}M(5)}^{5}$	$\left(\frac{1, -1}{3, -1}\right)$	$\left(\frac{2, 1}{-1, 3}\right)$	$\left(\frac{0, -1}{2, 0}\right)$	$\left(\frac{1, 2}{3, -1}\right)$	
(IV)	6	720	$\overline{G}_{M(3^2)}^{10}$	$\left(\frac{1, 0}{0, 1}\right)_-$	$\left(\frac{1, \sqrt{-1}}{0, 1}\right)_-$	$\left(\frac{0, 1}{1, 0}\right)_-$	$\left(\frac{-1, 1}{0, 1}\right)_-$	$\left(\frac{-1, 0}{0, 1}\right)_-$

ALTERNATING GROUPS $G_{\frac{1}{2}k!}$

	k	$\frac{1}{2}k!$	Group	E_1	E_2	E_3	E_4	
(V)	4	12	$G_{M(3)}^{4}$	$\left(\frac{1, 1}{0, 1}\right)$	$\left(\frac{0, -1}{1, 0}\right)$			
(VI)	5	60	$G_{M(3^2)}^{5}$	$\left(\frac{\rho, 0}{0, \rho^{-1}}\right)$	$\left(\frac{1, 1}{0, 1}\right)$	$\left(\frac{0, -1}{1, 0}\right)$		$(\rho^2+\rho+1=0)$
(VII)	5	60	$G_{M(5)}^{6}$	$\left(\frac{1, 1}{-1, 0}\right)$	$\left(\frac{1, 3}{1, 4}\right)$	$\left(\frac{1, 1}{0, -1}\right)$		
(VIII)	6	360	$G_{M(3^2)}^{10}$	$\left(\frac{1, -\sqrt{-1}}{0, 1}\right)$	$\left(\frac{0, 1}{1, 0}\right)$	$\left(\frac{-1, 1}{0, 1}\right)$	$\left(\frac{-1, 0}{0, 1}\right)$	

[2] Except for the group (IV) $\overline{G}_{M(3^2)}^{10}$. In this case the coefficients are marks of the $GF[3^2]$ and the substitution

$$\omega' = \frac{\alpha\bar{\omega} + \beta}{\gamma\bar{\omega} + \delta}$$

on the 10 marks ω — the 9 of the $GF[3^2]$ and ∞ — where $\bar{\omega}$ is the conjugate of ω with respect to the $GF[3^2]$ (§ 3 (48°) § 4; $\bar{\infty} = \infty$), is denoted by

$$\left(\frac{\alpha, \beta}{\gamma, \delta}\right)_-,$$

or $(\alpha, \beta; \gamma, \delta)_-$. (The $G_{\frac{1}{2}M(3^2)}^{10}$ is *not* a symmetric G_{61}.)

(6°) The regular tetrahedron, octahedron, icosahedron have groups G_{12}, G_{24}, G_{60} of rotation into themselves which are holoedrically isomorphic to the $G^4_{\frac{1}{2}4!}$, $G^4_{4!}$, $G^5_{\frac{1}{2}5!}$. Accordingly these latter groups and all corresponding group-forms are called the tetrahedron, octahedron, icosahedron groups.

(7°) We notice (for use in § 15 (2°)) that the tetrahedron group $G_{12}\{E_1, E_2\}$ $[I = E_1^2 = E_2^2 = (E_1E_2)^3]$ contains a self-conjugate four-group $[I, K = E_2, L = E_1E_2E_1^2, M = KL = E_1^2E_2E_1]$ and an operator $U = E_1$ such that

$$U^3 = I\ ,\quad UK = LU\ ,\quad UL = MU\ ,\quad UM = KU\ .$$

§ 2. THE GALOIS-FIELD OF ORDER $s = q^n$, $GF[s]$

Suppose that we have a system of s distinct symbols or *marks*,[3] $\mu_1, \mu_2, \cdots \mu_s$ (s being some finite positive integer), and suppose that these marks may be combined by the four fundamental operations of algebra—addition, subtraction, multiplication, and division—these operations being subject to the ordinary abstract *operational identities* of algebra

$$\mu_i + \mu_j = \mu_j + \mu_i\ ;\quad \mu_i\mu_j = \mu_j\mu_i\ ;\quad (\mu_i + \mu_j)\mu_k = \mu_i\mu_k + \mu_j\mu_k\ ;\quad \text{etc.}$$

and that when the marks are so combined the results of these operations are in every case uniquely determined and belong to the system of marks. Such a system of marks we shall call a *field of order s*, using the notation $F[s]$.

We are led at once to seek *To determine all such fields $F[s]$ of order s.*

This determination is the subject of this section, § 2.

The most familiar instance of such a field of order $s = q =$ a prime is the system of q incongruous classes (modulo q) of rational integral numbers a.

Galois discovered an important generalization[4] of the preceding field. Let $F_n(X)$, a rational integral function of the indeterminate X of degree n with integral coefficients, c_i, $c_n = +1$,

$$F_n(X) \equiv \sum_{i=0}^{n} c_i X^i\ ,$$

be irreducible, modulo q. Then the Galois-field of order $s = q^n$, $GF[q^n]$, consists of the system of q^n incongruous classes (modulis $q, F_n(X)$) of rational integral functions of X with integral coefficients. In this $GF[q^n]$ there exist *primitive roots;* the $q^n - 1$ successive powers of a primitive root are the $q^n - 1$ marks of the field (0 excluded).

The Galois-field $GF[q^n]$ is uniquely defined for every $q =$ prime, $n =$ positive integer; that is:

$F_n(X)$ which are irreducible (mod. q) do exist;

The $GF[q^n]$ is independent of the particular irreducible $F_n(X)$ used in its construction.

[3] It is necessary that all *quantitative* ideas should be excluded from the concept *marks*. Note that the signs $>$, $<$ do not occur in the theory.

[4] For the details of this Galois theory, see GALOI "Sur la théorie des nombres," *Bulletin des sciences math. matiques de M. Férussac*, Vol. XIII (1830), p. 428; reprinted in *Journal de mathématiques pures et appliquées*, Vol. XI (1846), pp. 398-407; SERRET, *Algèbre supérieure*, fifth edition, Vol. II, pp. 122-39; and JORDAN, *Substitutions*, pp. 14-18.

Assuming now (nothing but) *the existence of a field of order s* $F[s]$, I proceed to establish its fundamental properties, and prove in particular (40°) that:

Every existent field $F[s]$ *is the abstract form of a Galois-field* $GF[q^n]$; $s = q^n$.

The purely abstract form here given to the theory would seem to fit it best for immediate use wherever it can with advantage be introduced.

Naturally in many details my deduction of the properties of the $F[s]$ runs parallel to the work of Galois, Serret, and Jordan in investigating the $GF[q^n]$. I forbear to give closer references. For *ultimate existence-proofs* I fall back (22°, 38°, 39°) on the Galois theory. This sharp separation of the necessary properties of the field $F[s]$ *if existent* from the details of the various existence-proofs I consider highly desirable.

Def.—Any rational function of any number of indeterminates $X_1, X_2 \cdots X_k$, is said to *belong to the field* or to *be of the field*, if it has as coefficients marks of the field. An equation between two such functions is said likewise to belong to the field or to be of the field.

A rational integral function of any number of indeterminates belonging to the field is called *irreducible in the field* when it is not identically[5] the product of two or more such functions belonging to the field.

(1°) The theorems of ordinary algebra concerning rational functions of indeterminates hold for functions of our field; in particular, the algorithm for determination of the highest common factor of two rational integral functions of the indeterminate X.

(2°) The s marks $\mu_1 - \mu_1$, $\mu_2 - \mu_2$, $\cdots$, $\mu_s - \mu_s$ are equal; this mark is written $\mu_{(0)}$ or 0.

(3°) In division the mark $\mu_{(0)} = 0$ may never be the divisor.

(4°) The $s-1$ marks $\frac{\mu_i}{\mu_i}(\mu_i \neq \mu_{(0)})$ are equal; this mark is written $\mu_{(1)}$ or 1.

(5°) $\mu_i + \mu_{(0)} = \mu_i$ for every μ_i.

(6°) $\mu_{(0)}\,\mu_i = \mu_i\,\mu_{(0)} = \mu_{(0)}$ for every μ_i.

(7°) $\mu_{(1)}\,\mu_i = \mu_i\,\mu_{(1)} = \mu_i$ for every μ_i.

(8°) $\mu_i \mu_j = \mu_{(0)} = 0$ only if $\mu_i = \mu_{(0)} = 0$ or $\mu_j = \mu_{(0)} = 0$.

Def.—c being any positive integer, we denote the mark $\mu_{(1)} + \mu_{(1)} + \cdots + \mu_{(1)}$ or $1 + 1 + \cdots + 1$ (c terms) by $\mu_{(c)}$ or c (but by the latter notation c only when it is perfectly clear that by c a *mark* c is meant).

$$\mu_{(0)} - \mu_{(1)} = \mu_{(-1)} \ .$$

$$\mu_{(-1)} + \mu_{(-1)} + \cdots + \mu_{(-1)}\ (c \text{ terms}) = \mu_{(-c)} \ .$$

Thus we have defined the marks for *all* integral values c. These are called the *integral marks* of the $F[s]$. (See footnote at beginning of § 2, and (17°).)

(9°) $\mu_{(c_1)} + \mu_{(c_2)} = \mu_{(c_1+c_2)}$; $\mu_{(c_1)} - \mu_{(c_2)} = \mu_{(c_1-c_2)}$; $\mu_{(c_1)}\,\mu_{(c_2)} = \mu_{(c_1 c_2)}$.

(10°) $\mu_i + \mu_i + \cdots + \mu_i\ (c \text{ terms}) = \mu_{(c)}\,\mu_i = c\mu_i$.

[5] In the indeterminates.

(11°) The equation belonging to the field

$$f_k(X) = 0 ,$$

where $f_k(X)$ is a rational integral function of X of degree k, has *in the field* at most k roots, unless it is an identity in X when every mark of the field is a root.

(12°) If we have in the field an identity in X

$$f_k(X) \equiv f_{l_1}(X) \cdot f_{l_2}(X) \qquad (k = l_1 + l_2) ,$$

and if the equations $f_k(X) = 0, f_{l_1}(X) = 0$ have in the field k' and l_1' roots respectively, then the equation $f_{l_2}(X) = 0$ must have as roots the remaining $k' - l_1'$ roots of $f_k(X) = 0$.

Here $$k' \leqq k, l_1' \leqq l_1, k' - l_1' \leqq k - l_1 .$$

In particular, if $k' = k$, then $l_1' = l_1$, for from $l_1' < l_1$ would follow $k' - l_1' > k - l_1$.

(13°) For every mark ν of the field $F[s]$ there exist (because there are only s marks in the field) positive integral solutions c of the equation

$$c\nu = 0 , \quad \text{or } \mu_{(c)}\nu = 0 .$$

The smallest such solution is called the additive-period of the mark ν. All the solutions are multiples of this additive-period.

(14°) The additive-period of the mark $\mu_{(0)} = 0$ is 1.

(15°) The additive-period c_ν of any mark $\nu \neq \mu_{(0)}$ is the smallest positive integer c for which (7°, 13°)

$$\mu_{(c)} = \mu_{(c)}\mu_{(1)} = \mu_{(0)} ,$$

that is, *is the additive-period* $c_{\mu_{(1)}}$ of the mark $\mu_{(1)}$ or 1. All marks $\nu \neq \mu_{(0)}$ *have the same additive-period* c. This integer c is called the *modulus* of the field $F[s]$.

(16°) *This common additive-period or modulus* c *is a prime* q. For if c were composite, $c = dd'$ $(d < c, d' < c)$, we should have (9°, 13°)

$$\mu_{(c)} = \mu_{(0)} , \quad \mu_{(c)} = \mu_{(d)}\mu_{(d')} = \mu_{(0)} , \quad \mu_{(d)} \neq \mu_{(0)} ,$$

whence $\mu_{(d')} = \mu_{(0)}$, while from $d' < c$ follows $\mu_{(d')} \neq \mu_{(0)}$.

(17°) The marks $c = \mu_{(c)}$ for $c = 0, 1, 2, \cdots (q-1)$ are distinct; the mark $q = \mu_{(q)} = \mu_{(0)} = 0$. The integral marks are thus "*to be taken modulo* q." (This inheres in the concept *marks* and is not indicated in the notation.) These q integral marks form a field $F[q^1]$ (*the abstract form of the well-known field of rational integers taken modulo* q).

(18°) μ being any mark $\neq \mu_{(0)}$, the q marks $c\mu$ $(c = 0, 1, 2 \cdots (q-1))$ are distinct and form an additive-group $[\mu]$ with the basis-system μ, in the sense that the sum of any two of these marks is a third of the same system

$$c_1\mu + c_2\mu = (c_1 + c_2)\mu ,$$

or

$$\mu_{(c_1)}\mu + \mu_{(c_2)}\mu = \mu_{(c_1 + c_2)}\mu .$$

Def.—Any h marks ν_i $(i = 1, 2, \cdots h)$ of the field $F[s]$ are called linearly independent with respect to the field $F[q]$ (17°) if the equation

$$\sum_{i=1}^{h} c_i \nu_i = 0 ,$$

where the c_i's are marks of the $F[q]$, can be satisfied only in case every $c_i = 0$.

(19°) Any h marks ν_i $(i = 1, 1, \cdots h)$ linearly independent with respect to the $F[q]$ give rise to the q^h distinct marks of the field

$$\sum_{i=1}^{h} c_i \nu_i . \qquad \left(\begin{matrix}\text{Every } c_i \text{ has the values} \\ 0, 1, \cdots, (q-1)\end{matrix}\right) .$$

Def.—These q^h marks form *an additive-group* $[\nu_1, \nu_2, \cdots, \nu_h]$ *of rank*[6] h with respect to the field $F[q]$ of which the h marks $\nu_1 \cdots \nu_h$ form the *basis-system.*[6] The additive-group is transformed into itself when every mark is multiplied by a mark $(\neq 0)$ of the $F[q]$.

If from any h' linearly independent marks ν_j', $(j = 1, 2, \cdots, h')$ of this additive-group we form the additive-group $[\nu_1', \nu_2', \cdots, \nu_{h'}']$ of rank h', this group is entirely contained in the original additive-group. Any $h + 1$ marks of an additive-group of rank h are linearly dependent.

Any mark of the field $F[s]$ not in the additive-group $[\nu_1, \nu_2, \cdots, \nu_h]$ of rank h forms with the h marks of the basis-system a system of $h + 1$ linearly independent marks, the basis-system of an additive-group of rank $h + 1$.

(20°) Our field $F[s]$ of *finite* order s may therefore be exhibited as an additive-group of some *finite* rank n; *hence* s *must have the form* $s = q^n$.

(21°) Any field included within our field $F[s = q^n]$ may likewise be exhibited as an additive-group of rank $l \leqq n$.

This rank l of the $F[q^l]$ thought of as an additive-group is called also the rank of the field $F[q^l]$ itself. It turns out (26°) that the rank l of the included field $F[q^l]$ is a divisor of the rank n of the including field $F[q^n]$.

(22°) Any mark μ of the field $F[s = q^n]$ satisfies an equation of the form

$$f_k(X) \equiv \sum_{i=0}^{k} c_i X^i = 0 \qquad (c_k = 1) ,$$

where the expression $f_k(X)$ belongs to and is irreducible in the field $F[q^l]$. The positive integer k, the degree of the equation, is called the rank of the mark μ with respect to the $F[q^l]$.

For consider the successive powers μ^i $(i = 0, 1, 2, \cdots)$ of the μ. A linear relation with coefficients belonging to the $F[q^l]$ holds certainly between any $n + 1$ marks of the $F[s = q^n]$ (20°, 19°) and so between the first $n + 1$ powers μ^i. Suppose that for our mark μ such a linear relation does not hold between the first k powers (and so not between the first k' powers $k' \leqq k$), but does hold between the first $k + 1$ powers.

[6] FROBENIUS UND STICKELBERGER, "Ueber Gruppen von vertauschbaren Elementen," *Journal für die reine und angewandte Mathematik*, Vol. LXXXVI (1878), pp. 217-62, use these terms (p. 219).

We have $$\sum_{i=0}^{k} c_i' \mu^i = 0 ,$$

where the c_i' belong to the $F[q]$ and $c_k' \neq 0$; divide by c_k' and set c_i for c_i'/c_k'; we have

$$\sum_{i=0}^{k} c_i \mu^i = 0 ,$$

where the c_i belong to the $F[q]$ and $c_k = 1$; whence the equation

$$f_k(X) \equiv \sum_{i=0}^{k} c_i X^i = 0$$

is satisfied by the mark $X = \mu$.

The expression $f_k(X)$ so determined does belong to the $F[q]$ and is in it irreducible.[7] For if we had the decomposition $f_k(X) \equiv f_{k_1}(X) f_{k_2}(X)$ in the field $F[q]$, then $X = \mu$ would satisfy either $f_{k_1}(X) = 0$ or $f_{k_2}(X) = 0$, neither of which equations can be satisfied by μ, since the first $k_1 + 1$, $k_2 + 1 < k + 1$ powers of μ are linearly independent with respect to the $F[q]$.

Following Galois (see the reference given above), we recognize in this *additive-group* $[\mu^0 = 1, \mu^1, \cdots \mu^{k-1}]$ *of rank k the abstract form of a Galois-field of order* q^k, $GF[q^k]$.

(23°) *Every mark of our field* $F[s = q^n]$ *serves to define such a Galois-field*, the field of lowest rank k in which it lies. Every field in which it lies has its rank k' a multiple of k (26°).

Def.—Any h marks ν_i $(i = 1, 2, \cdots h)$ of the field $F[q^n]$ are called linearly independent with respect to any included field $F[q^l]$ $(l \leqq n)$, if the equation

$$\sum_{i=1}^{h} \gamma_i \nu_i = 0 ,$$

where the γ_i are marks of the field $F[q^l]$, can be satisfied only in case every $\gamma_i = 0$.

(24°) Any such system of h marks gives rise to q^{hl} distinct marks of the field obtained from the general form

$$\sum_{i=1}^{h} \gamma_i \nu_i$$

by letting the h γ_i's run independently through the series of marks of the $F[q^l]$. These q^{hl} marks form an *additive-group* $[\nu_1, \nu_2, \cdots \nu_h | F[q^l]]$ with the *basis-system* $\nu_1, \nu_2, \cdots \nu_h$ and the *field of reference* $F[q^l]$, of *rank h with respect to the* $F[q^l]$.

(25°) Any mark ν_{h+1} of the field $F[q^n]$ but not in this additive-group (24°) forms with the h marks of the basis-system a system of $h + 1$ marks linearly independent with respect to the $F[q^l]$, and thus leads to an additive-group of rank $h + 1$ with respect to the $F[q^l]$.

For the equation $$\sum_{i=1}^{h+} \gamma_i \nu_i = 0$$

is impossible, *first*, if $\gamma_{h+1} = 0$, since the h marks $\nu_1, \nu_2, \cdots \nu_h$ are by hypothesis

[7] $f_k(X)$ is reducible in the field $F[s]$; it has the factor $X - \mu$.

linearly independent with respect to the $F[q^l]$, and, *secondly*, if $\gamma_{h+1} \neq 0$, since this equation would lead (by multiplying by $-1/\gamma_{h+1}$, and by substituting for the marks $-\gamma/\gamma_{h+1}$ which belong to the *field* $F[q^l]$ the marks γ_i' respectively) to the equation

$$\nu_{h+1} = \sum_{i=1}^{h} \gamma_i' \nu_i ,$$

which would contradict the hypothesis that the ν_{h+1} is not in the additive-group $[\nu_1, \nu_2, \cdots, \nu_h | F[q^l]]$.

(26°) Our field $F[s = q^n]$ of *finite* order $s = q^n$ may be exhibited with respect to any included field $F[q^l]$ of order q^l as an additive-group of some *finite* rank h; $s = q^n = q^{hl}$; $n = hl$.

The rank l of any field $F[q^l]$ included in the field $F[q^n]$ of rank n is a divisor of n. The quotient h is the rank of the including field $F[q^n]$ with respect to the included field $F[q^l]$; $n = hl$.

(27°) For every mark $\nu \neq \mu_{(0)}$ of the field $F[s = q^n]$ there exist (because there are only s marks in the field) positive integral solutions e of the equation

$$\nu^e = \mu_{(1)} = 1 .$$

The smallest such solution, say e, is called the *multiplicative-period* or *exponent* of the mark ν; ν is said to *belong to this exponent* e. The e marks $\nu^0 = 1, \nu^1, \nu^2, \cdots, \nu^{e-1}$ are distinct, and form a multiplicative-group.

(28°) If two marks ν_1, ν_2 belong to exponents e_1, e_2 respectively which are relatively prime, their product belongs to the exponent $e_1 e_2$, and the marks

$$\nu_1^{d_1} \nu_2^{d_2} \qquad \begin{pmatrix} d_1 = 0, 1, 2, \cdots, (e_1 - 1) \\ d_2 = 0, 1, 2, \cdots, (e_2 - 1) \end{pmatrix}$$

are $e_1 e_2$ distinct marks.

(29°) The $s - 1 = q^n - 1$ marks $\mu \neq 0$ may be thought of as the elements of a multiplicative-group of order $s - 1$. The *period* of the element ν is its exponent e. Whence e is a divisor of $s - 1 = q^n - 1$.

The equation of the field $F[s = q^n]$

$$X^e - 1 = 0 ,$$

where e is the exponent of some mark ν has in the field at most e roots (11°) (not having the root $X = 0 = \mu_{(0)}$), and in fact it has the e roots ν^i $(i = 0, 1, 2, \cdots (e-1))$.

(30°) The equation of the field

$$X^{s-1} - 1 = X^{q^n - 1} - 1 = 0$$

is satisfied by every one of the $s - 1$ marks $\nu \neq 0$, since the exponent of every mark ν is a divisor of $s - 1$.

(31°) The equation of the field

$$X^s - X = X^{q^n} - X = 0$$

is satisfied by every mark ν of the field $F[s=q^n]$. Hence the decomposition in the $F[s=q^n]$

$$X^{q^n}-X\equiv\prod_{i=1}^{q^n}(X-\mu_i)\ .$$

This is the generalization for the $F[q^n]$ of Fermat's Theorem for the $F[q^1]$.

(32°) Converse of (29°). f being any divisor of $s-1=q^n-1$ the equation

$$X^f-1=0$$

has in the $F[s=q^n]$ exactly f roots.

For let $s-1=fg$. We have the identity in X in the field $F[q^1]$ and so in the field $F[s=q^n]$.

$$X^{s-1}-1\equiv(X^f-1)(X^{(g-1)f}+X^{(g-2)f}+\cdots+X^{2f}+X^f+1)\ ;$$

whence (30°, 12°) the desired conclusion follows.

(33°) In particular, if $s-1=q^n-1=p_1^{h_1}p_2^{h_2}\cdots p_k^{h_k}$, where the p's are the distinct prime factors of $s-1$, the equation

$$X^{p_i^{h_i}}-1=0$$

for i any integer of the series $1, 2, \cdots k$ has in the field $F[s=q^n]$ $p_i^{h_i}$ roots ν. The exponent e of every one of these roots is a divisor of $p_i^{h_i}$ and hence is of the form $p_i^{h_i'}$ $(h_i'\leqq h_i)$. Of these roots $p_i^{h_i-1}$ belong to exponents which are factors of $p_i^{h_i-1}$, namely, the $p_i^{h_i-1}$ roots of the equation

$$X^{p_i^{h_i-1}}-1=0\ .$$

The remaining $p_i^{h_i}-p_i^{h_i-1}=p_i^{h_i}\left(1-\frac{1}{p_i}\right)$ roots belong to the exponent $p_i^{h_i}$ itself.

Whence, by multiplication of marks belonging to the various exponents $p_i^{h_i}$ for $i=1, 2, \cdots, k$, we obtain in all

$$\prod_{i=1}^{k}p_i^{h_i}\left(1-\frac{1}{p_i}\right)=\phi(s-1)=\phi(q^n-1)$$

distinct marks belonging by (28°) to the exponent

$$\prod_{i=1}^{k}p_i^{h_i}=s-1=q^n-1\ .$$

[Here $\phi(t)$ denotes, as usual, the number of integers less than and relatively prime to the positive integer t.]

Thus, *the* $s-1=q^n-1$ *marks* $(\neq 0)$ *of the field* $F[s=q^n]$ *are the* $s-1$ *powers of a mark* ρ *belonging to the exponent* $s-1$, or say, *of a primitive root* ρ *of the equation* $X^{s-1}-1=0$, *or of the field* $F[s=q^n]$ *itself. The multiplicative-group of the* $s-1$ *marks is cyclic.*

(34°) Similarly: Any equation of the form

$$X^f-1=0\ ,$$

where f is any divisor of $s-1=q^n-1$, has in the $F[q^n]$ f roots (32°), of which $\phi(f)$ are primitive roots.

ρ being a primitive root of the equation

$$X^{s-1}-1=0 ,$$

then $\rho^{\frac{s-1}{f}}$ is a primitive root of the equation

$$X^f-1=0 .$$

(35°) All the results reached may be applied to any field $F[q^l]$, in particular to any $F[q^l]$ included within the $F[q^n]$, where then (26°) l is a divisor of n. The marks of such a $F[q^l]$ are the q^l roots of the equation (31°, 32°)

$$X^{q^l}-X=X(X^{q^l-1}-1)=0 .$$

Our field $F[q^n]$ containing one $F[q^l]$ contains *no other* $F[q^l]$.

The converse of (35°) is true; see (39°).

(36°) Every mark ν ($\neq 0$) of the $F[q^n]$ is the root of an equation

$$F_k(X)\equiv\sum_{i=1}^{k}c_iX^i=0 \qquad (c_k=1) ,$$

belonging to and irreducible in the $F[q]$ of degree k equal to the rank of the mark with respect to the $F[q]$; see (22°).

The greatest common divisor of $X^{q^n}-X$ and $F_k(X)$ both of which belong to the $F[q]$ does itself also belong to the $F[q]$; but $F_k(X)$ is irreducible in the $F[q]$; the divisor is accordingly $F_k(X)$ itself, or some mark independent of X. The process necessary to determine this divisor may however be interpreted *also in the* $F[q^n]$, in which case $X-\nu$ is recognized as a common factor (31°, 22°, footnote). Whence in the $F[q]$ $X^{q^n}-X$ is exactly divisible by every such expression $F_k(X)$. Here k is a divisor of n (26°, 22°).

(37°) First converse of (36°). Every factor $F_k(X)$ of degree k of $X^{q^n}-X$ which belongs to and is irreducible in the $F[q]$ has in the $F[q^n]$ k linear factors (31°, 32°)

$$F_k(X)\equiv c_k\prod_{i=1}^{k}(X-\nu_i) .$$

The mark ν_1 defines (23°) a Galois-field $GF[q^k]$ of order q^k contained in the $F[q^n]$. Whence k is a divisor of n (22°).

(38°) Second converse of (36°). Every expression $F_k(X)$ of degree k, a divisor of n, belonging to and irreducible in the $F[q]$ occurs as a factor of $X^{q^n}-X$. For every such $F_k(X)$ serves (by the Galois theory) to define a $GF[q^k]$; whence the $F_k(X)$ is a factor of $X^{q^k}-X=X(X^{q^k-1}-1)$ (36°) and thus of

$$X(X^{q^n-1}-1)=X^{q^n}-X .$$

(39°) Galois-fields $GF[p^k]$ exist (being by the Galois theory defined by such an

$F_k(X)$, (38°)) for every prime q and integer k. *Our* $F[q^n]$ *contains one* (38°, 37°, 23°) *and only one* (35°) $GF[q^k]$ *for every* k *a divisor of* n, *and no other fields whatever* (26°, 35°). *The marks of such an included* $GF[q^k]$ *are the* q^k *roots of the equation*

$$X^{q^k} - X = 0 \ .$$

k is the rank of the field $GF[q^k]$ (21°).

(40°) In particular, for $k = n$,

Every existent field $F[s]$ *is the abstract form of a Galois-field* $GF[q^n]$; $s = q^n$.

I use always hereafter the notation $GF[q^k]$ instead of $F[q^k]$.

(41°) The marks common to two included fields of ranks k_1 and k_2 respectively constitute a third field, and indeed of rank k where k is the greatest common divisor of k_1 and k_2 (39°, 36°).

(42°) The field of lowest rank containing two included fields of rank k_1 and k_2 respectively is the field of rank k' where k' is the least common multiple of k_1 and k_2.

(43°) The mark ν ($\neq 0$) of the $GF[q^n]$ has the exponent e (27°), satisfies the equation $F_k(X) = 0$ (22°) belonging to and irreducible in the $GF[q]$, and defines the $GF[q^k]$ (23°, 39°). By the method of proof of (36°): $F_k(X)$ is an exact divisor of $X^e - 1$ in the $GF[q]$; $X^e - 1$ is an exact divisor of $X(X^{q^k-1} - 1) = X^{q^k} - X$ (since e is a factor of $q^k - 1$ (29°)); $X^{q^k} - X$ is an exact divisor of $X^{q^n} - X$ (since the rank k is a divisor of the rank n (26°). (This accords with (36°).)

(44°) The exponent e of a mark ν ($\neq 0$) and the rank k of the mark ν with respect to the $GF[q]$, or, what is the same thing, the rank k of the $GF[q^k]$ defined by the mark ν, are thus related:

e is a divisor of $q^k - 1$ (29°), and of $q^{k'} - 1$ only for k' a multiple of k.

e being a divisor of $q^k - 1$ and of $q^{k'} - 1$ is a divisor of $q^l - 1$, where l is the greatest common divisor of k and k'. Now this l is k itself, and so k' is a multiple of k. For, since e is a divisor of $q^l - 1$, $l \leqq k$, $X^e - 1$ is a divisor of $X^{q^l-1} - 1$ and of $X^{q^l} - X$; the mark ν lies in the $GF[q^l]$ (12°, 29°, 32°); l is a multiple of k (23°, 26°), and so in fact equal to k.

In particular, a primitive root (34°) of the equation

$$X^{q^k-1} - 1 = 0 \ ,$$

where k is a divisor of n, is of rank k. For its e is $q^k - 1$.

(45°) Similarly:

$F_k(X)$ is an exact divisor of $X^e - 1$, and of $X^{e'} - 1$ only for e' a multiple of e.

$F_k(X)$ is an exact divisor of $X^{q^k-1} - 1$, and of $X^{q^{k'}-1} - 1$ only for k' a multiple of k.

(46°) Similarly, using also the method of (36°):

The mark ν is a root of the equation $X^e - 1 = 0$, and of $X^{e'} - 1 = 0$ only for e a multiple of e.

The mark ν is a root of the equation $X^{q^k-1} - 1 = 0$, and of $X^{q^{k'}-1} - 1 = 0$ only for k' a multiple of k.

(47°) The equation

$$F_k(X) = 0$$

is in the $FG[q^k]$ completely reducible, having the roots

$$X = \nu\ ,\quad \nu^q\ ,\quad \nu^{q^2}, \cdots, \nu^{q^{k-1}} (\nu^{q^k} = \nu)\ .$$

These k marks are distinct, for if two were equal, the mark ν would satisfy an equation $X^{q^{k'}} - X = 0$ with $k' < k$, contrary to (46°).

That they are roots of the equation depends upon the following lemma:

Lemma.—The rational integral function

$$F_k(X) \equiv \sum_{i=0}^{k} c_i X_i\ ,$$

belongs to the $GF[q^l]$ and satisfies the equation

$$\{F_k(X)\}^{q^h} \equiv F_k(X^{q^h})\ ,$$

where h is any positive integer.

This is proved for the general h, if proved for $h = 1$.

$$\{F_k(X)\}^q \equiv \left\{ \sum_{i=0}^{k} c_i X^i \right\}^q \equiv \sum_{i=0}^{k} c_i^q X^{iq} \equiv \sum_{i=0}^{k} c_i (X^q)^i \equiv F_k(X^q)\ ,$$

since the multinomial coefficients for the product terms vanish in the $GF[q]$ owing to the presence of the factor q, and since $c_i^q = c_i$ (Fermat's Theorem; (31°)).

(48°) The mark λ being now *any* mark in the $GF[q^k]$ it defines a $GF[q^l]$, l a certain divisor of k. Then λ satisfies the equation

$$X^{q^l} - X = 0\ .$$

Def.—The k marks

$$\lambda' = \lambda^{q^0}\ ,\quad \lambda^{q^1}\ ,\quad \lambda^{q^2}\ , \ldots,\ \lambda^{q^{k+1}} (\lambda^{q^k} = \lambda)$$

are called *conjugate with respect to the* $GF[q]$.

These k conjugate marks are, in view of $\lambda^{q^l} = \lambda$, the l marks

$$\lambda^1 = \lambda^{q^0}\ ,\quad \lambda^{q^1}\ ,\quad \lambda^{q^2}\ , \ldots,\ \lambda^{q^{l-1}}\ ,$$

k/l times repeated. These l marks are the roots of an equation

$$F_l(X) \equiv \prod_{i=0}^{l-1} (X - \lambda^{q^i}) = 0\ ,$$

belonging to and irreducible in the $GF[q]$ (22°, 47°).

The expression

$$F_k(X) \equiv \prod_{i=0}^{k-1} (X - \lambda^{q^i})$$

in the $GF[q]$ has the decomposition

$$F_k(X) \equiv \{F_l(X)\}^{\frac{k}{l}}\ .$$

It would be interesting, and for other allied investigations necessary, to study in detail the properties of the $GF[q^n]$ with respect to *any* included $GF[q^l]$, as we have studied the properties with respect to the $GF[q^1]$.

Concerning squares and not-squares in the $GF[q^n]$.

(49°) Let ρ be a primitive root of the $GF[q^n]$, that is, of the equation (33°)

$$X^{s-1} - 1 \equiv X^{q^n-1} - 1 = 0 .$$

(*a*) If $q > 2$, and so $s - 1 = \text{even} = 2t$, then $\rho^t = -1 \neq +1$; the $\left\{ \begin{matrix} \text{even} \\ \text{odd} \end{matrix} \right\}$ powers of ρ are $\left\{ \begin{matrix} \text{squares} \\ \text{not-squares} \end{matrix} \right\}$; every square $\sigma = \rho^{2h}$ has two square roots ρ^h and $\rho^{h+t} = -\rho^h$. With respect to the multiplication and division of squares and not-squares the well-known laws of the theory of numbers [that is, for the particular case of the $GF[q], n = 1$] hold.

(*b*) If $q = 2$, and so $s - 1 = \text{odd} = 2t + 1$, then ρ^2 is also a primitive root of the $GF[q^n = 2^n]$ (since 2 is prime to $s - 1$); every mark is a square, and has only one square root. (We notice that $-1 = +1$ in this $GF[2^n]$.)

Thus in the $GF[q^n]$

$$\text{If } \left\{ \begin{matrix} q > 2 \\ q = 2 \end{matrix} \right\} \text{ there are } \left\{ \begin{matrix} \frac{1}{2}(s-1) \text{ squares, } \frac{1}{2}(s-1) \text{ not-squares.} \\ s - 1 = 2^n - 1 \text{ squares.} \end{matrix} \right\}$$

(50°) If $q > 2$, the not-squares of any $GF[q^l]$ are in an including $GF[q^n]$ not-squares or squares according as the rank $n/l = h$ of the $GF[q^n]$ with respect to the $GF[q^l]$ is odd or even.

$$\rho_1 = \rho^u \text{ where } u = \frac{q^n - 1}{q^l - 1} \text{ is a primitive root of the } GF[q^l] \text{ (34°).}$$

The marks ($\neq 0$) of the $GF[q^l]$ are given by $\rho_1^v = \rho^{uv}$ $(v = 0, 1, \cdots (l-1))$. Let ρ_1^v be in $GF[q^l]$ a not-square; v is odd; $\rho_1^v = \rho^{uv}$ is in $GF[q^n]$ a not-square or a square according as uv, that is, as u, is odd or even, that is, in fact, according as $h = n/l$ is odd or even. For by the equation

$$u = \frac{q^n - 1}{q^l - 1} = \frac{q^{hl} - 1}{q^l - 1} = \sum_{i=0}^{h-1} q^{li} ,$$

we exhibit u as the sum of h odd terms.

(51°) In the $GF[q^n]$ the additive-group of lowest rank containing all the squares[8] (or not-squares) is the $GF[q^n]$ itself. This is true for $q = 2$ (49°). For $q > 2$, if this were not true, the $\frac{1}{2}(q^n - 1)$ squares and the 0 would constitute a $GF[q'^{n'} = \frac{1}{2}(q^n + 1)]$ where $q' = q$, *quâ* the fundamental additive-period (15°), and this is impossible.

[8] BURNSIDE (*loc. cit.*, p. 118) is the first to state this theorem. His proof is inadequate.

§ 3. THE GALOIS-FIELD OF ORDER $s=q^{2n}$

Notation.—The $GF[q^{2n}]$ contains one $GF[q^n]$ (§ 2, 39°). Hereafter in this paper I shall use the small Roman letters $a, b, c, \ldots$ to denote integers and also marks of the $GF[q]$, the small Greek letters $\alpha, \beta, \gamma, \ldots$ to denote marks of the $GF[q^n]$, and the large Roman letters $A, B, C, \ldots$ to denote marks of the $GF[q^{2n}]$.

Def.—In the $GF[q^{2n}]$ the two marks A, B where $B=A^{q^n}$, $A=B^{q^n}$ (since $A^{q^{2n}}=A$) are called *conjugate with respect to the* $GF[q^n]$. The notation $\overline{A}$ for the conjugate of A is used.

(1°) If and only if A belongs to the $GF[q^n]$, does $\overline{A}=A$.

(2°) $\overline{AC}=\overline{A}\,\overline{C}$, $\overline{A^t}=(\overline{A})^t$, $\overline{\overline{A}}=A$, $\overline{\alpha A+\beta B+\gamma C}=\alpha\overline{A}+\beta\overline{B}+\gamma\overline{C}$.

(3°) Every mark A of the $GF[q^{2n}]$ and not of the $GF[q^n]$ is the root of an equation

$$F_2(X)\equiv X^2-\kappa X+\lambda=0\ ,$$

belonging to and irreducible in the $GF[q^n]$. The two roots are $X=A$ and $X=A^{q^n}=\overline{A}$.

For: $A+\overline{A}=K$ and $A\overline{A}=L$ belong to the $GF[q^n]$, since (2°, 1°)

$$\overline{K}=\overline{A+\overline{A}}=\overline{A}+A=K\ ,$$
$$\overline{L}=\overline{A\overline{A}}=\overline{A}A=L\ .$$

We may then set $A+\overline{A}=\kappa$, $A\overline{A}=\lambda$ and have in

$$X^2-\kappa X+\lambda=0$$

an equation belonging to the $GF[q^n]$ with the roots $X=A, \overline{A}$ and irreducible in the $GF[q^n]$ since its roots do not belong to $GF[q^n]$.

(4°) Converse of (3°). Every quadratic equation

$$F_2(X)\equiv X^2-\kappa X+\lambda=0$$

belonging to and irreducible in the $GF[q^n]$ is reducible in the $GF[q^{2n}]$, having as roots a pair of conjugate marks $A, \overline{A}$.

(*a*) There are in all q^{2n} distinct quadratic equations belonging to the $GF[q^n]$.

(*b*) Of these $\frac{1}{2}(q^{2n}+q^n)$ are reducible in the $GF[q^n]$, viz., q^n with equal and $\frac{1}{2}(q^n(q^n-1))$ with unequal roots.

(*c*) There are $\frac{1}{2}(q^{2n}-q^n)$ irreducible ones which are exactly the equations (3°) whose roots are respectively the $\frac{1}{2}(q^{2n}-q^n)$ pairs of conjugate marks $A, \overline{A}$.

Note that every mark β a not-square in the $GF[q^n]$ is a square in the $GF[q^{2n}]$ (§ 2, 50°).

(5°) Since q^n+1 is a divisor of $q^{2n}-1$, the equation

$$X^{q^n+1}-1=0$$

has in the $GF[q^{2n}]$ as roots the q^n+1 successive powers of a primitive root J (§ 2, 34°),

where $J = R^{q^n-1}$, R being a primitive root of the $GF[q^{2n}]$. Any mark A whose conjugate is its reciprocal

$$A\overline{A} = A^{q^n+1} = 1 ,$$

is thus a power of J and with its conjugate satisfies (3°) a quadratic equation of the form,

$$X^2 - \kappa X + 1 = 0 .$$

The powers of J which lie in the $GF[q^n]$ satisfy likewise the equation

$$X^{q^n-1} - 1 = 0 ,$$

and so the equation

$$X^2 - 1 = 0 ;$$

they are then $J^0 = +1$, and (for $q > 2$, q^n+1 even) $J^{\frac{1}{2}(q^n+1)} = -1$.

Thus there are $\left\{\begin{array}{l}\text{if } q > 2,\ \frac{1}{2}(q^n-1)\\ \text{if } q = 2,\ \frac{1}{2}q^n = 2^{n-1}\end{array}\right\}$ quadratic equations of the form

$$X^2 - \kappa X + 1 = 0 ,$$

which belong to and are irreducible in the $GF[q^n]$.

I write the one satisfied by J and $\overline{J} = J^{-1}$ thus

$$(X - J)(X - \overline{J}) \equiv X^2 - \theta X + 1 = 0 , \qquad (J;\ \theta)$$

thereby defining the mark θ of the $GF[q^n]$

$$\theta = J + J = J + J^{-1} .$$

(6°) In the $GF[q^{2n}]$ the mark J having the period $e = q^n+1$ defines (§ 2, 23° 39°) the $GF[q^{2n}]$ itself (§ 2, 44°).

(7°) In the $GF[q^n]$ the mark θ defines the $GF[q^n]$ itself. For let θ define the $GF[q^l]$ (l a divisor of n). The $GF[q^{2n}]$ contains a $GF[q^{2l}]$, in which the equation belonging to the $GF[q^l]$

$$X^2 - \theta X + 1 = 0 , \qquad (J;\ \theta)$$

is reducible (4°). Hence its root J belongs to the $GF[q^{2l}]$. Thus indeed $l = n$ (6°).

(8°) There are $\phi(q^n+1)$ primitive roots J and thus $\frac{1}{2}\phi(q^n+1)$ marks θ. We do not now need to inquire further into the properties of this system of marks θ.

(9°) Any mark A of the $GF[q^{2n}]$ may be written in one and only one way in the form

$$A = \gamma + \delta J .$$

(§ 2, 24°). Its conjugate is (2°, 5°)

$$\overline{A} = \gamma + \delta \overline{J} .$$

§ 4. DEFINITION OF THE GROUP $G^{q^n+1}_{M(q^n)}$

The abstract group $G_{M(q^n)}$ will be studied under three concrete substitution-group forms $G^{q^n+1}_{M(q^n)}$, $G'^{q^{2n}+1}_{M(q^n)}$, and $G''^{q^{2n}+1}_{M(q^n)}$. Indeed it will be now *defined* by its concrete form $G^{q^n+1}_{M(q^n)}$.

We work in the $GF[q^n]$ with the mark ∞ adjoined. The mark ∞ shall have with respect to the $GF[q^n]$ operational properties strictly analogous to those of the algebraic symbol ∞ with respect to the totality of finite algebraic symbols.

Let the variable marks ω, ω' run through this series of q^n+1 marks. Let $\alpha, \beta, \gamma, \delta$ be any marks of the $GF[q^n]$ for which the *determinant* $\Delta = \alpha\delta - \beta\gamma \neq 0$. Then the linear fractional substitution

$$V: \quad \omega' = \frac{\alpha\omega + \beta}{\gamma\omega + \delta} \qquad (\alpha\delta - \beta\gamma = \Delta \neq 0) \tag{1}$$

makes correspond to every mark ω a certain mark ω', and indeed so that ω' takes every one of its $q^n + 1$ values, the *reciprocal substitution* being

$$V^{-1}: \quad \omega = \frac{\frac{\delta}{\Delta}\omega' - \frac{\beta}{\Delta}}{-\frac{\gamma}{\Delta}\omega' + \frac{\alpha}{\Delta}}. \tag{2}$$

V effects then a definite permutation of the $q^n + 1$ marks ω and will be thought of as a notation for a substitution-operation on those $q^n + 1$ marks.

The notations

$$\left(\frac{\alpha, \beta}{\gamma, \delta}\right), \quad (\alpha, \beta; \gamma, \delta) \tag{3}$$

are used for the substitution V.

Corresponding to the formulæ

$$\begin{gathered} (V'') \quad \omega'' = \frac{\alpha''\omega' + \beta''}{\gamma''\omega' + \delta''}, \qquad (V') \quad \omega' = \frac{\alpha'\omega + \beta'}{\gamma'\omega + \delta'}, \\ (V) \quad \omega'' = \frac{(\alpha''\alpha' + \beta''\gamma')\omega + (\alpha''\beta' + \beta''\delta')}{(\gamma''\alpha' + \delta''\gamma')\omega + (\gamma''\beta' + \delta''\delta')}, \end{gathered} \tag{4}$$

we have the formula of composition or multiplication of substitutions

$$\begin{gathered} V''V' = V; \\ (\alpha'', \beta''; \gamma'', \delta'')(\alpha', \beta'; \gamma', \delta') = (\alpha''\alpha' + \beta''\gamma', \alpha''\beta' + \beta''\delta'; \gamma''\alpha' + \delta''\gamma', \gamma''\beta' + \delta''\delta'). \end{gathered} \tag{5}$$

The determinant of the product of two substitutions is the product of the determinants of the substitutions.

The totality of all such distinct substitutions of determinant $+1$ constitutes the substitution-group $G^{s+1}_{M(s)} = G^{q^n+1}_{M(q^n)}$ of order $M(s) = M(q^n)$ on the $s + 1$ marks ω.

The two substitutions

$$V = (\alpha, \beta; \gamma, \delta), \quad V_\mu = (\mu\alpha, \mu\beta; \mu\gamma, \mu\delta) \qquad \left(\begin{smallmatrix} \alpha\delta - \beta\gamma = \Delta \neq 0 \\ \mu \neq 0 \end{smallmatrix}\right) \tag{6}$$

are the same in fact. Their determinants are $\Delta = \alpha\delta - \beta\gamma$, $\Delta_\mu = \mu^2\Delta$. (a) Case $q > 2$. The marks ($\neq 0$) are half squares and half not-squares (§ 2, 49°); and Δ^{-1} or $\Delta^{-1}\rho$ is a square, according as Δ is or is not a square (ρ being a primitive root of the $GF[q^n]$). By choosing then $\mu = \pm\sqrt{\Delta^{-1}}$ or $\pm\sqrt{\Delta^{-1}\rho}$ according as Δ is or is not a square, V_μ has its determinant $\Delta_\mu = 1$ or ρ respectively. (b) Case $q = 2$. Every

mark ($\neq 0$) is a square (§ 2, 49°). By choosing then $\mu = \sqrt{\Delta^{-1}}$ (uniquely defined in the $GF[q^n = 2^n]$), V_μ has its determinant $\Delta_\mu = 1$.

These forms of the substitution for which the determinant is 1 or ρ $(q > 2)$; 1 $(q = 2)$ are called *normal* forms of the substitutions.

Every substitution has exactly, if $q > 2$, two normal forms, or, if $q = 2$, one normal form:

$$\begin{array}{ll} (q>2) & (\alpha, \beta;\ \gamma, \delta) = (-\alpha, -\beta;\ -\gamma, -\delta) \qquad (\alpha\delta - \beta\gamma = 1 \text{ or } \rho) \\ (q=2) & (\alpha, \beta;\ \gamma, \delta) \qquad (\alpha\delta - \beta\gamma = 1) \end{array} . \quad (7)$$

It is easily proved that the equation of the $GF[s = q^n]$, $\alpha\delta - \beta\gamma = \epsilon$, in which ϵ is a fixed mark $\neq 0$, has $(s-1)s(s+1)$ solutions $(\alpha, \beta, \gamma, \delta)$.

Thus: $(q > 2)$. There are $\frac{1}{2}s(s^2-1)$ substitutions $(\alpha, \beta;\ \gamma, \delta)$ having $\Delta = \alpha\delta - \beta\gamma =$ square (in normal form, $\Delta = 1$) and $\frac{1}{2}s(s^2-1)$ having $\Delta =$ not-square (in normal form, $\Delta = \rho$).

$(q = 2.)$ There are s (s^2-1) substitutions $(\alpha, \beta;\ \gamma, \delta)$ (in normal form $\Delta = 1$).

Thus clearly *the order* $M(s)$, $s = q^n$, *of the group* $G^{s+1}_{M(s)}$ (embracing *the totality of substitutions with determinant* 1) *is*[9]

$$\frac{s(s^2-1)}{2;\ 1} = \frac{q^n(q^{2n}-1)}{2;\ 1} = M(s) = M(q^n) \qquad (q>2;\ q=2). \quad (8)$$

The group of all the substitutions with determinants not 0 has the order $(2; 1)\ M(s)$, according as $(q > 2;\ q = 2)$. For $q > 2$ the $G_{2M(s)}$ contains the $G_{M(s)}$ as a self-conjugate subgroup of index 2. Since every mark Δ $(\Delta \neq 0)$ of the $GF[q^n]$ is a square in the $GF[q^{2n}]$ (§ 2, 50°), *the* $G_{2M(s)}$ $(q > 2)$ *is a subgroup of the* $G_{M(s^2 = q^{2n})}$ *of the* $GF[q^{2n}]$. Hence, we easily extend (section by section) the investigation of the subgroups of the $G_{M(s)}$ to the subgroups of the $G_{(2;\ 1)\ M(s)}$.

§ 5. DEFINITION OF THE GROUPS $G'^{q^{2n}+1}_{M(q^n)}$, $G''^{q^{2n}+1}_{M(q^n)}$, TWO "IMAGINARY" FORMS OF THE $G_{M(q^n)}$

We work in the $GF[q^{2n}]$ with a mark ∞ adjoined, and let the variable marks W, W' run through this series of $q^{2n} + 1 = s^2 + 1$ marks. (s is used hereafter uniformly for q^n.)

We consider the group $G^{s^2+1}_{(2;\ 1)\ M(s^2)}$ $(q > 2;\ q = 2)$ of all substitutions of the form

$$\left(W' = \frac{AW+B}{CW+D}\right) \text{ or } \left(\frac{A, B}{C, D}\right) \text{ or } (A, B;\ C, D) \qquad (AD - BC \neq 0) . \quad (1)$$

This group contains the subgroup $G^{s^2+1}_{(2;\ 1)\ M(s)}$ of all substitutions of the form

$$\left(W' = \frac{\alpha W+\beta}{\gamma W+\delta}\right) \text{ or } \left(\frac{\alpha, \beta}{\gamma, \delta}\right) \text{ or } (\alpha, \beta;\ \gamma, \delta) \qquad (\Delta = \alpha\delta - \beta\gamma \neq 0) , \quad (2)$$

[9] We shall need to discriminate frequently between the cases $q > 2$, $q = 2$. The compact notation used for such discrimination should cause no confusion.

which is holoedrically isomorphic with the substitution-group $G^{s+1}_{(2;1)M(s)}$ (§4) on the $s+1$ marks ω; indeed, it is an intransitive group on the s^2+1 marks W, the $s+1$ marks ω forming one system of intransitivity.

The group $G^{s^2+4}_{(2;1)M(s^2)}$ contains also the substitution

$$R=(J,1;\bar{J},1) \tag{3}$$

of determinant $J-\bar{J}\neq 0$ (§3, 1°, 5°). We have (§3, 5°)

$$J^2=\theta J-1;\ \bar{J}^2=\theta\bar{J}-1\ . \tag{4}$$

$$J\bar{J}=1;\ J+\bar{J}=\theta;\ (J-\bar{J})^2=\theta^2-4\neq 0\ . \tag{5}$$

$$R^{-1}=\left((J-\bar{J})^{-1},\ -(J-\bar{J})^{-1};\ -\bar{J}(J-\bar{J})^{-1},\ J(J-\bar{J})^{-1}\right)\ . \tag{6}$$

R transforms[10] the group $G^{s^2+1}_{(2;1)M(s)}\{V\}$ into an holoedrically isomorphic group $G'^{s^2+1}_{(2;1)M(s)}\{V'\}=R\{V\}R^{-1}=\{V'=RVR^{-1}\}$, where

$$V=(\alpha,\beta;\ \gamma,\delta) \qquad (\Delta=\alpha\delta-\beta\gamma\neq 0)\ ; \tag{7}$$

$$V'=\begin{pmatrix}A,&B\\ \bar{B},&\bar{A}\end{pmatrix}=\begin{pmatrix}\kappa+\lambda J\ ,&\mu+\nu J\\ \mu+\nu\bar{J}\ ,&\kappa+\lambda\bar{J}\end{pmatrix} \qquad (\Delta'=A\bar{A}-B\bar{B}=\Delta)\ , \tag{8}$$

$$\kappa=\delta+\frac{(\beta-\gamma)\theta-2(\alpha-\delta)}{\theta^2-4}\ , \tag{9}$$

$$\lambda=\ +\frac{(\alpha-\delta)\theta-2(\beta-\gamma)}{\theta^2-4}\ ,$$

$$\mu=\ -\frac{(\beta-\gamma)\theta-2(\alpha-\delta)}{\theta^2-4}\ ,$$

$$\nu=\beta-\frac{(\alpha-\delta)\theta-2(\beta-\gamma)}{\theta^2-4}\ ;$$

$$\Delta'=A\bar{A}-B\bar{B}=\kappa^2+\lambda^2-\mu^2-\nu^2+(\kappa\lambda-\mu\nu)\theta=\alpha\delta-\beta\gamma=\Delta\ . \tag{10}$$

This group $G'^{s^2+1}_{(2;1)M(s)}$ includes *every* substitution of the form V' (8). The V is determined from the V' by the formulæ

$$\alpha=+\kappa-\mu+\lambda\theta\ , \tag{11}$$
$$\beta=+\lambda+\nu\ ,$$
$$\gamma=-\lambda+\nu+\mu\theta\ ,$$
$$\delta=+\kappa+\mu\ ;$$

$$\Delta=\alpha\delta-\beta\gamma=\kappa^2+\lambda^2-\mu^2-\nu^2+(\kappa\lambda-\mu\nu)\theta=A\bar{A}-B\bar{B}=\Delta'\ . \tag{12}$$

The group $G'^{s^2+1}_{M(s)}\{V'\}$ (8) ($\Delta'=1$) is the first "imaginary" form of the $G_{M(s)}$. For $n=1$, $q>2$ this form was introduced (by Serret, Mathieu, and then) by Gierster, *loc. cit.*, p. 327, and indeed, as we have done for the general case, by introducing the broader group $G^{q^2+1}_{2M(q^2)}$, within which $G^{q^2+1}_{M(q)}$ ($\Delta=1$) and the $G'^{q^2+1}_{M(q)}$ ($\Delta'=1$) are conjugate

[10] R, V being two operators of a group, R *transforms* V into the conjugate operator $V'=RVR^{-1}$. This definition is preferable to the other, $V'=R^{-1}VR$, when as here in the $G^{s+1}_{M(s)}$ the operators are substitutions on the $s+1$ marks operating *from the right to the left*.

subgroups (*loc. cit.*, p. 331). Gierster (*loc. cit.*, p. 328) and Klein-Fricke (*loc. cit.*, p. 425) use transforming substitutions which depend upon the square root in the $GF[q^2]$ of a not-square in the $GF[q^1]$. Since, however, not-squares do not exist in $GF[s=q^n]$ with $q=2$, we have made use of a transforming substitution R of a different type which does exist for the general n with $q=2$ as well as with $q>2$.

The group $G^{s^2+1}_{(3;1)\,M(s^2)}$ contains the substitution

$$R'=(K, 0;\ 0, 1)\ , \tag{13}$$

where K is a particular square root of J, so that

$$K\bar{K}=-1\ ,\quad R'^{-1}=(-\bar{K}, 0;\ 0, 1)\ . \tag{14}$$

Under R' the group $G'^{s^2+1}_{(3;1)\,M(s)}\{V'\}$ (8) transforms into the holoedrically isomorphic group $G''^{s^2+1}_{(3;1)\,M(s)}\{V''\}$ of *all* substitutions of the form

$$V''=(A, B;\ -\bar{B}, \bar{A}) \qquad (\Delta''=A\bar{A}+B\bar{B}=\Delta)\ . \tag{15}$$

The group $G''^{s^2+1}_{M(s)}\{V''\}$ $(\Delta''=1)$ is the (new) second imaginary form[11] of the $G_{M(s)}$. This form is found more convenient than the first form (§§ 6, III, 15, 16), since it contains $T=(0, -1;\ 1, 0)$.

We notice the three corresponding substitutions:

$$V_\theta=(\theta, 1;\ -1, 0)\ ,\quad V'_\theta=V''_\theta=D^2_J=(J, 0;\ 0, \bar{J})\ , \tag{16}$$

where in general we write

$$D_\Delta=(A, 0;\ 0, 1)\ . \tag{16'}$$

Within the $G^{s^2+1}_{(3;1)\,M(s^2)}$ the three conjugate groups,

$$(a)\ G^{s^2+1}_{(3;1)M(s)}\ (2)\ ,\quad (b)\ G'^{s^2+1}_{(3;1)M(s)}\ (8)\ ,\quad (c)\ G''^{s^2+1}_{(3;1)M(s)}\ (15)$$

contain respectively all substitutions of non-vanishing determinant of the form

$$V=(\alpha, \beta;\ \gamma, \delta)\ ,\quad V'=(A, B;\ \bar{B}, \bar{A})\ ,\quad V''=(A, B;\ \bar{B}, \bar{A})\ . \tag{17}$$

The necessary and sufficient conditions that a substitution

$$U=(A, B;\ C, D)=(AM, BM;\ CM, DM) \qquad (AD-BC\neq 0;\ M\neq 0)$$

belong to the respective groups are:

$$\begin{aligned}
&(a)\quad AB^s=A^sB\ ,\quad AC^s=A^sC\ ,\quad AD^s=\ \ A^sD\ ,\\
&\qquad CD^s=C^sD\ ,\quad DB^s=D^sB\ ,\quad BC^s=\ \ B^sC\ ;\\
&(b)\quad A^{s+1}=D^{s+1}\ ,\quad B^{s+1}=C^{s+1}\ ,\quad AC^s=\ \ D^sB\ ;\\
&(c)\quad A^{s+1}=D^{s+1}\ ,\quad B^{s+1}=C^{s+1}\ ,\quad AC^s=-D^sB\ .
\end{aligned} \tag{18}$$

Thus, for instance, the substitution

$$(1, 1;\ 1, -1)=(\sqrt{\rho}, \sqrt{\rho};\ \sqrt{\rho}, -\sqrt{\rho})$$

of determinant -2, -2ρ belongs (for $q>2$) both to the real and to the second imaginary $G_{2M(s)}$, while it belongs to the real or to the second imaginary $G_{M(s)}$ according as -2 is a square or a not-square in the $GF[s]$.

[11] In the recent automorphic-function literature a similar type of substitution is prominent. For instance, FRICKE, "Zur gruppentheoretische Grundlegung der automorphen Functionen," *Mathematische Annalen*, Vol. XLII (1893), p. 564. This second imaginary form of the group was independently discovered by Dickson during the year 1899.

§6. THE INDIVIDUAL OPERATORS AND THE LARGEST CYCLIC AND COMMUTATIVE SUBGROUPS OF THE $G_{M(s)}$

To summarize at once the conclusions of this section:

Of the $G_{M(s)}$ every operator (the identity excepted) determines and lies in one and only one largest[12] *commutative subgroup. These subgroups constitute three different sets, the groups of each set being conjugate with one another under the $G_{M(s)}$.*

(I) $s+1$ *conjugate commutative* $G_{s=q^n}$. *These* s^2-1 *operators are all of period* q. *For* $q=2$ *these are all conjugate operators. For* $q>2$ *they separate into two sets of* $\frac{1}{2}(s^2-1)$ *conjugate operators, The* $q-1$ *operators of a cyclic group* $G_q(q>2)$ *belong* $\left\{\begin{array}{l} n \text{ odd, half to one and half to the other} \\ n \text{ even, all to the same} \end{array}\right\}$ *set of conjugate operators.*

(II)[12] $\frac{1}{2}s(s+1)$ *conjugate cyclic groups* $G_{\frac{s-1}{2;1}}(q>2;\ q=2)$.

(III)[12] $\frac{1}{2}s(s-1)$ *conjugate cyclic groups* $G_{\frac{s+1}{2;1}}(q>2;\ q=2)$.

(IV)[12] *Two substitutions* $(A, B; C, D)$, $(A', B'; C', D')$, *of determinant 1 of the* $G_{M(s)}$ *in its real or first imaginary or second imaginary form* (§5) (*neither substitution being the identity*) *are conjugate if and only if* $(A+D)^2=(A'+D')^2$. *But—the substitutions of set I all have* $(A+D)^2=4$ *and for* $q>2$ *separate into two sets of conjugate substitutions.*

(V)[13] *For* $q>2$, *for the substitutions of set*

$$\left.\begin{array}{l}\text{(I)}^{14}\\ \text{(II)}\\ \text{(III)}\end{array}\right\}\ (A+D)^2-4 \text{ is } \left\{\begin{array}{l}0.\\ \text{a square in the } GF[s].\\ \text{a not-square in the } GF[s].\end{array}\right.$$

[For the cases $s=9$; 7 (the $G_{M(s)}$ being the 6!-symmetric group G_{360}; the simple group G_{168}) the cyclic groups (II); (III) of order 4 exist as stated, but every element of order 2 of such a cyclic group lies in and determines not merely this largest commutative subgroup of order 4 but two other four-groups, the three groups of order 4 lying in the dihedron group of order 8 whose cyclic base is the cyclic group in question. These two are the only cases in which an operator determines two or more "largest" commutative subgroups. This follows from the developments of the text in view of the fact that a non-commutative dihedron group of order $2d$ contains two commutative subgroups of order d only if $d=4$. The classification of the four-groups is made in § 9.]

The operators and groups of the three types will be discussed by considering the $G_{M(s)}$ in the concrete substitution-group form $G^{s+1}_{M(s)}$ for types I, II, and $G'^{s^2+1}_{M(s)}$ for type III.

[12] For the cases $s=q^1=5$; 3 (the $G_{M(s)}$ being the icosahedron G_{60}; the tetrahedron G_{12}) the groups (II); (III) above specified, viz., 15 conjugate G_2 under the G_{60}; 3 conjugate G_2 under the G_{12}, exist, but every one is contained in a *larger* commutative four-group, these constituting a system of (II) five conjugate commutative four-groups; (III) one commutative four-group.

[13] *Cf.* GIERSTER (*loc. cit.*, pp. 326, 327) and BURNSIDE (*loc. cit.*, pp. 122-4).

[14] The characterisation V (I) holds also for $q=2$.

I. *The operators of period* q. — Denote by S_β the substitution of the $G^{s+1}_{M(s)}$

$$S_\beta = (1, \beta;\ 0, 1)\ . \tag{1}$$

We have

$$S_{\beta_1} S_{\beta_2} = S_{\beta_1+\beta_2} = S_{\beta_2} S_{\beta_1}\ ;\ S_\beta{}^a = S_{a\beta} \tag{2}$$

$$S_\beta{}^q = S_{q\beta} = S_0 = I;\ S_\beta{}^{-1} = S_{-\beta} = S_\beta{}^{q-1}\ ; \tag{3}$$

where I denotes the identical substitution,

$$I = (1, 0;\ 0, 1)\ . \tag{4}$$

The totality of $s = q^n$ substitutions S_β constitutes a commutative group $G^{(\infty)}_s\ \{S_\beta\}$ of order $s = q^n$; it contains all and only the substitutions leaving the single mark $\omega = \infty$ invariant. Every substitution (except the identity) is of period q. There are $(s-1)/(q-1)$ cyclic G_q in the $G^{(\infty)}_s$.

To study the conjugacy of these substitutions and groups under the $G^{s+1}_{M(s)}$ we transform $S_\mu (\mu \neq 0)$ by $V = (\alpha, \beta;\ \gamma, \delta)$, and obtain

$$V S_\mu V^{-1} = \begin{pmatrix} 1 - \alpha\gamma\mu,\ \alpha^2\mu \\ -\gamma^2\mu,\ 1 + \alpha\gamma\mu \end{pmatrix}\ . \tag{5}$$

This transformed substitution belongs to the $G^{(\infty)}_s$ if and only if in V $\gamma = 0$, and in fact $V = (\alpha, \beta;\ 0, \alpha^{-1})$, does transform S_μ into $S_{\alpha^2\mu}$, while in particular any $S_\beta = (1, \beta;\ 0, 1)$ transforms S_μ into itself.

Within the $G^{s+1}_{M(s)}$ the substitution $S_\mu\ \{\mu \neq 0\}$ is self-conjugate in exactly the $G^{(\infty)}_s\ \{S_\beta\}$, while the $G^{(\infty)}_s$ is self-conjugate in exactly the $G^{(\infty)}_{\frac{s(s-1)}{2;\,1}}\{(\alpha, \beta;\ 0, \alpha^{-1})\}$ which contains all the substitutions leaving $\omega = \infty$ fixed. The order of this last group is $\dfrac{s(s-1)}{2;\,1}$, for α has in all $s-1$ values ($\neq 0$), and β has independently s values; every substitution is however counted twice if $q > 2$. The substitution S_μ is conjugate under the $G^{s+1}_{M(s)}$ with the substitutions $S_{\alpha^2\mu}$, *i. e.*, if $(q > 2;\ q = 2)$, with (only half; all) the $s-1$ substitutions of the $G^{(\infty)}_s$ (§ 2, 49°). If $q > 2$, the $s-1$ substitutions of the $G^{(\infty)}_s$ separate into two sets of $\frac{1}{2}(s-1)$ conjugate substitutions; under the $G_{2M(s)}$ they are however all conjugate, since by D_ρ (§ 4 (9)) S_1 transforms to S_ρ. The $q-1$ substitutions of a cyclic group $G_q\ \{S_{\alpha\mu}\}\ (\alpha \neq 0)$ belong half to one and half to the other set, if n is odd, since then only half the integral marks α are *in the* $GF[q^n]$ square (§ 2, 50°), while if n is even, they all belong to the same set, since all the marks α are in the $GF[q^n]$ squares.

In the $G^{s+1}_{M(s)}$ there are

$$\left\{ M(s) = \frac{s(s^2-1)}{2;\ 1} \right\} \div \frac{s(s-1)}{2;\ 1} = s + 1$$

conjugate commutative groups $G^{(\kappa)}_s$. Each of these is *defined* by any substitution lying in it (the identity excepted) as *the* group in which that substitution is self-conjugate. The $s+1$ groups have the identity in common, but otherwise have quite distinct substitutions all of period q, s^2-1 in all.

$G_s^{(\kappa)}$ is self-conjugate in a group $G^{(\kappa)}_{\frac{s(s-1)}{2;1}}$. These $s+1$ groups $G^{(\kappa)}_{\frac{s(s-1)}{2;1}}$ are under the $G_{M(s)}$ a set of conjugate groups. They are distinct, since $G^{(\infty)}_{\frac{s(s-1)}{2;1}}$ contains substitutions S_β lying in no other $G^{(\kappa)}_{\frac{s(s-1)}{2;1}}$.

II. *The operators of periods divisors of* $\frac{s-1}{2;1}$.—Denote by P the substitution of the $G^{s+1}_{M(s)}$

$$P=(\rho, 0;\ 0, \rho^{-1}) , \tag{6}$$

where ρ is a primitive root of the field $GF[s]$ (§2, 33°). We have as powers of P

$$P^\varrho=(\rho^\varrho, 0;\ 0, \rho^{-\varrho}) \qquad (\varrho=0, \pm 1, \pm 2, \ldots) \tag{7}$$

ρ belongs to the exponent $s-1$. The cyclic group generated by P has order $\frac{s-1}{2;1}$ $(q>2;\ q=2)$; we denote it by $G^{(\infty 0)}_{\frac{s-1}{2;1}}\{P^\varrho\}$, since it contains all and only the substitutions leaving $\omega=\infty$ and $\omega=0$ each fixed. The substitutions $(\alpha, \beta;\ \gamma, \delta)$, $(\alpha\delta-\beta\gamma=1)$ of this group are defined by the equations $\beta=0$, $\gamma=0$. We write also

$$P_\alpha=(\alpha, 0;\ 0, \alpha^{-1})=P_{-\alpha} \qquad (\alpha\neq 0) . \tag{7'}$$

This group $G^{(\infty 0)}_{\frac{s-1}{2;1}}$ contains a substitution of period two if and only if $s=q^n$ has the form $s=q^n=4h+1$; in this case

$$P^h=P^{\frac{s-1}{4}}=(\sqrt{-1}, 0;\ 0, -\sqrt{-1}) \tag{8}$$

exists and has the period two.

Any substitution V of the $G^{s+1}_{M(s)}$

$$V=(\alpha, \beta;\ \gamma, \delta) \qquad (\alpha\delta-\beta\gamma=1) \tag{9}$$

transforms $P^\varrho \neq I$ $(\rho^\varrho \neq \pm 1$; and so $\rho^\varrho-\rho^{-\varrho}\neq 0)$ into

$$VP^\varrho V^{-1}=\begin{pmatrix} \alpha\delta\rho^\varrho-\beta\gamma\rho^{-\varrho}, & -\alpha\beta(\rho^\varrho-\rho^\varrho) \\ \gamma\delta(\rho^\varrho-\rho^{-\varrho}), & \alpha\delta\rho^{-\varrho}-\beta\gamma\rho^\varrho \end{pmatrix} . \tag{10}$$

This transformed substitution belongs to the cyclic group $G^{(\infty 0)}_{\frac{s-1}{2;1}}\{P^\varrho\}$ if in V $\alpha\beta=0$ and $\gamma\delta=0$. We have also $\alpha\delta-\beta\gamma=1$. Two cases arise.

First case: $\beta=\gamma=0$. $V=(\alpha, 0;\ 0, \alpha^{-1})$ itself belongs to the cyclic group $G^{(\infty 0)}_{\frac{s-1}{2;1}}$ and of course transforms every P^ϱ of the group into itself.

Second case: $\alpha=\delta=0$. $V=(0, \beta;\ -\beta^{-1}, 0)$ transforms P^ϱ into $P^{-\varrho}$, which is distinct from P^ϱ unless P^ϱ is of period two.

Within the $G_{M(s)}$ the cyclic $G^{(\infty 0)}_{\frac{s-1}{2;1}}$ is self-conjugate in exactly the dihedron group $G^{(\infty 0)}_{2\frac{s-1}{2;1}}$ composed of the totality of substitutions having the forms $(\alpha, 0;\ 0, \alpha^{-1})$, $(0, \beta;\ -\beta^{-1}, 0)$.

Within the $G_{M(s)}$ a substitution P^σ is self-conjugate in exactly the $G^{(\infty\,0)}_{\frac{s-1}{2;\,1}}$, except in the case $s = q^n = 4h+1$, in which $P^{\frac{s-1}{4}}$ is self-conjugate in exactly the dihedron $G^{(\infty\,0)}_{2\frac{s-1}{2}}$; this dihedron group is commutative only if it is a four-group ($s = q^1 = 5$).

In the $G_{M(s)}$ there are $\left\{ M(s) = \frac{s(s^2-1)}{2;\,1} \right\} \div 2\frac{s-1}{2;\,1} = \frac{1}{2}s(s+1)$ conjugate cyclic groups $G^{(\kappa\lambda)}_{\frac{s-1}{2;\,1}} = G^{(\lambda\kappa)}_{\frac{s-1}{2;\,1}}$ $(\kappa \neq \lambda)$. Each of these is *defined* by any substitution lying in it (the identity excepted) as *the largest* cyclic group containing that substitution. The $\frac{1}{2}s(s+1)$ groups have the identity in common, but otherwise have quite distinct substitutions, of periods divisors of $\frac{s-1}{2;\,1}$, in all

$$\frac{s \cdot s+1}{2}\left(\frac{s-1}{2;\,1}-1\right) = \frac{s(s+1)\,(s-3;\ s-2)}{4;\ 2}$$

substitutions.

In the $G_{M(s)}$ there are $M(s) \div \frac{s-1}{2;\,1} = s\,(s+1)$ substitutions conjugate to P^σ of which two lie in every $G^{(\kappa\lambda)}_{\frac{s-1}{2;\,1}}$ (for instance, in $G^{(\infty\,0)}_{\frac{s-1}{2;\,1}}$ lie P^σ and $P^{-\sigma}$). However, for $s = q^n = 4h+1$, there are only $\frac{1}{2}s\,(s+1)$ substitutions conjugate to $P^{\frac{s-1}{4}}$, one lying in every $G^{(\kappa\lambda)}_{\frac{s-1}{2}}$.

$G^{(\kappa)}_{\frac{s(s-1)}{2;\,1}}$ and $G^{(\lambda)}_{\frac{s(s-1)}{2;\,1}}$ have $G^{(\kappa\lambda)}_{\frac{s-1}{2;\,1}}$ in common. $G^{(\infty)}_{\frac{s(s-1)}{2;\,1}}$ is made up of $G^{(\infty)}_{s}$ and the $s\ G^{(\infty\,\kappa)}_{\frac{s-1}{2;\,1}}$ (κ any $\neq 0$); S_β transforms $G^{(\infty\,\kappa)}_{\frac{s-1}{2;\,1}}$ to $G^{(\infty\,\kappa+\beta)}_{\frac{s-1}{2;\,1}}$.

III. *The operators of periods divisors of* $\frac{s+1}{2;\,1}$.—Denote by Q the substitution of the $G^{\prime\, s^n+1}_{M(s)}$ (§ 5 (16), $\Delta' = 1$)

$$(Q = J,\ 0;\ 0,\ \bar{J}), \tag{11}$$

where J is a primitive root of the equation $X^{s+1} = 1$ and $\bar{J} = J^{-1}$ (§ 3, 5°). We have as powers of Q

$$Q^\sigma = (J^\sigma,\ 0;\ 0,\ \bar{J}^\sigma) \qquad (\sigma = 0, \pm 1, \pm 2, \ldots).$$

J belongs to the exponent $s+1$. The cyclic group generated by Q has order $\frac{s+1}{2;\,1}$ $(q > 2;\ q = 2)$; denote it by $G^{*}_{\frac{s+1}{2;\,1}}\{Q^\sigma\}$. The substitutions $(A,\ B;\ -\bar{B},\ \bar{A})$ $(A\bar{A} + B\bar{B} = 1)$ of this group are defined by the equation $B = 0 = \bar{B}$; see (§ 3, 5°).

This group $G^{*}_{\frac{s+1}{2;\,1}}$ contains a substitution of period two if and only if $s = q^n$ has the form $s = q^n = 4k-1$; in this case

$$Q^k = Q^{\frac{s+1}{4}} = (\sqrt{-1},\ 0\ ;\ 0,\ -\sqrt{-1}) \tag{12}$$

exists and has the period two.

We notice particularly that in the $G_{M(s)}$ operations of period two are always present, being all of the type I, II, or III, according as q is even $(=2)$, or (q odd) q^n of the form $q^n = 4h+1$ or $q^n = 4k-1$.

Any substitution V of the $G^{\prime\, \frac{s^2+1}{2;\,1}}_{M(s)}$

$$V = (A, B;\ -\overline{B}, \overline{A}) \qquad (A\overline{A}+B\overline{B}=1) \tag{13}$$

transforms $Q^\sigma \neq I$ ($J^\sigma \neq \pm 1$; and so $J^\sigma - \overline{J}^\sigma \neq 0$) into

$$VQ^\sigma V^{-1} = \begin{pmatrix} A\overline{A}J^\sigma + B\overline{B}\overline{J}^\sigma , & -AB(J^\sigma - \overline{J}^\sigma) \\ -\overline{A}\overline{B}(J^\sigma - \overline{J}^\sigma) , & A\overline{A}\overline{J}^\sigma + B\overline{B}J^\sigma \end{pmatrix}. \tag{14}$$

This transformed substitution belongs to the cyclic group $G^*_{\frac{s+1}{2;\,1}}\{Q^\sigma\}$ if in V $AB=0$ and $\overline{A}\,\overline{B}=0$. We have also $A\overline{A}+B\overline{B}=1$.

Two cases arise.

First case: $B=\overline{B}=0$. $V=(A, 0;\ 0, \overline{A}=A^{-1})$ itself belongs to the cyclic group $G^*_{\frac{s+1}{2;\,1}}$ and, of course, transforms every Q^σ of the group into itself.

Second case: $A=\overline{A}=0$. $V=(0, B;\ -\overline{B}=-B^{-1}, 0)$ transforms Q^σ into $Q^{-\sigma}$, which is distinct from Q^σ unless Q^σ is of period two.

Within the $G_{M(s)}$ the cyclic $G^*_{\frac{s+1}{2;\,1}}$ is self-conjugate in exactly the dihedron group $G^*_{2\frac{s+1}{2;\,1}}$ composed of the totality of substitutions having the forms $(A, 0; 0, A^{-1})$, $(0, B; -B^{-1}, 0)$, where A and B are any powers of J.

Within the $G_{M(s)}$ a substitution Q^σ is self-conjugate in exactly the $G^*_{\frac{s+1}{2;\,1}}$, except in the case $s=q^n=4k-1$, in which the $Q^{\frac{s+1}{4}}$ is self-conjugate in exactly the dihedron $G^*_{2\frac{s+1}{2}}$; this dihedron group is commutative only if it is a four-group ($s=q^1=3$).

In the $G_{M(s)}$ there are $\left\{ M(s)=\frac{s(s^2-1)}{2;\,1} \right\} \div 2\frac{s+1}{2;\,1} = \frac{1}{2}s(s-1)$ cyclic groups $G_{\frac{s+1}{2;\,1}}$ conjugate to $G^*_{\frac{s+1}{2;\,1}}$. Each of these is *defined* by any substitution lying in it (the identity excepted) as *the largest* cyclic group containing that substitution. The $\frac{1}{2}s(s-1)$ groups have the identity in common, but otherwise have quite distinct substitutions, of periods divisors of $\frac{s+1}{2;\,1}$, in all

$$\frac{s\,.\,s-1}{2}\left(\frac{s+1}{2;\,1}-1\right) = \frac{s(s-1)\,(s-1;\,s)}{4;\,2}$$

substitutions.

In the $G_{M(s)}$ there are $M(s) \div \frac{s+1}{2;\,1} = s(s-1)$ substitutions conjugate to Q^σ of which two lie in every $G_{\frac{s+1}{2;\,1}}$ (in $G^*_{\frac{s+1}{2;\,1}}$, for instance, lie Q^σ and $Q^{-\sigma}$). However, for $s=q^n=4k-1$, there are only $\frac{1}{2}s(s-1)$ substitutions conjugate to $Q^{\frac{s+1}{4}}$, one lying in every $G_{\frac{s+1}{2;\,1}}$.

We have now enumerated all the individual operators of the $G_{M(s)}$, and likewise all the cyclic and largest commutative [14a] subgroups; for

$$1+(s^2-1)+\frac{s(s+1)(s-3;s-2)}{4;\ 2}+\frac{s(s-1)(s-1;s)}{4;\ 2}=\frac{s(s^2-1)}{2;\ 1}=M(s)\ .$$

(The identity is not enumerated under I, II, or III, and so is counted separately.)

We find similarly that the $G_{2M(s)}$ $(q>2)$ contains exactly the identity, s^2-1 substitutions of period q, and substitutions conjugate to the various powers of D_ρ (§ 4 (9); $D_\rho^2=P$) and of D_J (§ 5 (16); $D_J^2=Q$):

$$1+(s^2-1)+\frac{s(s+1)(s-2)}{2}+\frac{s(s-1)(s)}{2}=s(s^2-1)=2M(s)\ .$$

It remains to prove the Theorems IV and V.

Obviously, if under a substitution V of the $G_{M(s)}^{s+1}$ any three marks ω are fixed, then V is the identity I. The substitution V $(V\neq I)$ may then be separated into three classes according as they leave exactly one mark, two distinct marks, or no mark fixed. These three classes are precisely the three sets I, II, and III.

Under transformation $(A+D)^2$ is invariant. (The transforming substitution may be any substitution of the $G_{(2;\,1)\,M(s^2)}^{s^2+1}$.) To see in how far $(A+D)^2$ is a characteristic invariant for a system of substitutions conjngate under the $G_{M(s)}^{s+1}$, we need (by I, II, III) consider only the representative substitutions of such systems

$$\text{(I)}\quad S_\beta=(1,\beta;0,1)\ ;\quad \text{(II)}\quad P^\sigma=(\rho^\sigma,0;0,\rho^{-\sigma})\ ;\quad \text{(III)}\quad Q^\sigma=(J^\sigma,0;0,\overline{J}^\sigma)\ . \tag{15}$$

These are all of the form

$$V=(A,B;\ 0,D)\qquad {}_{(AD=1)}\ . \tag{16}$$

Two particular substitutions U_1, U_2 of the form (16) have the same invariant,

$$(A_1+D_1)^2=(A_2+D_2)^2\ , \tag{17}$$

if and only if

$$(A_1,D_1)=(A_2,D_2),\ (D_2,A_2),\ (-A_2,-D_2)\text{ or }(-D_2,-A_2)\ . \tag{18}$$

U_1 and U_2 belong then to the same set I, II, III. If they belong to set I, they always have the same invariant 4, but are not always conjugate (Theorem I). If, however, they belong to set II or to set III and have the same invariant, they are always conjugate; this appears from the considerations introduced in the proof of Theorems II and III.

Theorem IV has been proved.

The truth of theorem V appears at once from the consideration of the representative substitutions (15), in the light as to (III) of § 3.

The characterization V(I) holds also in the case $q=2$.

Substitutions of period 2 for q any are fully characterized by the property $\alpha+\delta=0$; however for $q=2$ the identity also satisfies the condition $\alpha+\delta=0$.

[14a] See the remark in brackets near the beginning of this § 6.

§7. EXTENSION OF THE $G_S^{(\infty)}$ $\{S_\beta = (1, \beta; 0, 1,)\}$ BY ANY UNIMODULAR SUBSTITUTION $V = (a, \beta; \gamma, \delta)$ $(\gamma \neq 0)$ TO THE $G_{M(s)}^{s+1}$, SYSTEMS OF GENERATORS OF THE $G_{M(s)}^{s+1}$ AND $G_{(3;\,1)M(s)}^{s+1}$

We consider the group $G\{U\}$ of all binary matrices

$$U = \begin{pmatrix} a, b, \\ c, d, \end{pmatrix} = (a, b, c, d) \qquad (ad - bc = 1) , \tag{1}$$

whose elements, a, b, c, d belong to a (finite or infinite) field and are subject only to the condition that $ad - bc = 1$.

We introduce

$$T = (0, -1, 1, 0) , \quad S_h = (1, h, 0, 1) , \quad S_h T = E_h = (h, -1, 1, 0) , \tag{2}$$

and have then

$$U_{(d \neq 0)} = E_{(b-1)d^{-1}} E_{-d} E_{-(c+1)d^{-1}} , \tag{3}$$

$$U_{(d=0,\ \text{and so}\ bc=-1)} = E_{t+rb} E_{-c} E_b E_{rc+w} , \tag{4}$$

where in (4) r is arbitrary and t and w are connected only by the equation

$$tc - wb + 1 = a . \tag{5}$$

The group $G\{S_h\}$ is then extended by T to the group $G\{U\}$.

More generally, the group $G\{S_h\}$ is extended by *any* particular matrix $U = V$ with $c \neq 0$ to the group $G\{U\}$, for

$$T = S_{1-ac^{-1}} V S_{c^{-2}-(a+d)c^{-1}} V S_{1-dc^{-1}} . \tag{6}$$

The theorem implied by the caption[15] is an obvious modification of a particular case — for the $GF[s]$[16]—of the theorem just proved.

The group $G\{U\}$ of unitary matrices U is of course extended by the matrices

$$D_d = (d, 0, 0, 1) \qquad (d \neq 0) \tag{7}$$

to the group $\overline{G}\{U\}$ of all matrices U of non-vanishing determinant. In view of the relation

$$D_d S_1 D_d^{-1} = S_d \tag{8}$$

the group $\overline{G}\{U\}$ is generated by the matrices D_d, S_1, and T.

When the fundamental field is the $GF[s]$ with the primitive root ρ, so that $d = \rho^e$, the matrix D_ρ generates the matrices D_d,

$$D_d = D_\rho^e , \tag{9}$$

and so the $\overline{G}\{U\}$ is generated by D_ρ, S_1, and T. Similarly[16] the group $\overline{G}\{U\}$ of all matrices U of determinant a square in the $GF[s]$ is generated by D_{ρ^2}, and S_1, and T.

Hence, for our groups $G_{M(s)}^{s+1}$, $G_{(3;\,1)M(s)}^{s+1}$ we have the respective systems[17] of three generators :

[15] This development of the theorem for the $G_{M(s)}^{s+1}(s=q^n)$ for the general n involves of necessity essential modifications of the development for $n=1$ (KLEIN-FRICKE, *loc. cit.*, pp. 452, 459).

[16] We need also §2, 51*.

[17] BURNSIDE (*loc. cit.*, pp. 117, 118) is the first to exhibit these systems of generators. He works directly with the fractional substitutions. His proof as to the $G_{M(s)}^{s+1}$ rests upon the lemma of §2, 51* of this paper, of which his proof was inadequate.

$$G^{s+1}_{M(s)}\ ; \quad D_{\rho^2} = P = (\rho, 0; 0, \rho^{-1})\ , \quad S_1 = (1, 1; 0, 1)\ , \quad T = (0, -1; 1, 0)\ ; \tag{10}$$

$$G^{s+1}_{(2;1)M(s)}\ ; \quad D_\rho = (\rho, 0; 0, 1)\ , \qquad S_1 = (1, 1; 0, 1)\ , \quad T = (0, -1; 1, 0)\ , \tag{11}$$

for the second group is obtained by extending the first by $D\rho$, and $D_{\rho^2} = D^2_\rho$.

§ 8. EVERY $G_{M(s)}$ $(s = q^n \neq 2^1, 3^1)$ IS A SIMPLE GROUP

A self-conjugate subgroup G_d $(d > 1)$ of the $G^{s+1}_{M(s)}$ must contain all the operators of at least one system of operators conjugate under the $G^{s+1}_{M(s)}$.

If the G_d contain one operator of set I, then it contains all operators conjugate with it and so (§ 6, I) all operators S_β where β is either any square or any not-square. Then the G_d contains all the operators S_β, $\beta =$ any (§ 2, 51°), and indeed the $s+1$ conjugate groups G_s (§ 6, I). Then the G_d is the $G_{M(s)}$ itself (§ 7), since it contains the G^∞_s $\{S_\beta\}$ and an operator $V = (\alpha, \beta; \gamma, \delta)$ with $\gamma \neq 0$.

If the G_d contain one operator

$$P^\sigma = (\rho^\sigma, 0;\ 0, \rho^{-\sigma})$$

of set II, then it contains the conjugate (§ 7, IV) operator

$$V = (\rho^{-\sigma}, \beta;\ 0, \rho^\sigma) \qquad (\beta \neq 0)\ ,$$

and then the product $S_{\beta\rho^\sigma} = \rho^\sigma V$, which is of set I. Thus the G_d is the $G_{M(s)}$ itself.

We now consider a self-conjugate G_d containing no operators of sets I or II. Except in the cases $s = 2^1$, 3^1 such a G_d turns out to be precisely $G_{d=1}$ = identity itself. Thus the theorem of the caption of § 8 is proved.

We treat this case[18] by the diophantine considerations employed in the Congress paper (pp. 238–42) for the general case. Since

$$M(s) = (2; 1) \cdot s \cdot \frac{s-1}{2;1} \cdot \frac{s+1}{2;1}\ , \tag{1}$$

d a divisor of $M(s)$ and prime to s and $\frac{s-1}{2;1}$ (by the Cauchy-Sylow theorem) must be a divisor of $(2; 1)\left(\frac{s+1}{2;1}\right)$, so that

$$d = 2^t c_+,\ c_+ = \left[\frac{s+1}{2;1}; d\right],\ 2^t = 1 \text{ or } 2;1, \tag{2}$$

where as usual $[u, v]$ denotes the greatest common divisor of the two positive integers u and v. Further (by § 6, III) the G_d contains and is made up of $\frac{1}{2}s(s-1)$ cyclic G_{d_+}, one from each of the conjugate cyclic $G_{\frac{s+1}{2;1}}$. Hence

$$d = 1 + \tfrac{1}{2}s(s-1)(d_+ - 1) = -\frac{s+1}{2;1} \cdot \frac{s-2}{1;2} + \tfrac{1}{2}s(s-1)d_+\ . \tag{3}$$

[18] BURNSIDE's treatment (*loc. cit.*, pp. 126, 132) of this third case fails either if his $\alpha + \delta = x^t = 0$ or if $q = 2$. As a result of these errors he overlooks the exceptional cases $s = q^n = 3^1, 2^1$.

Hence d_+ is a divisor of $\frac{s+1}{2;1}$ and of d, and so of c_+, and further c_+ is a divisor of $\frac{s+1}{2;1}$ and of d, and so not of $\frac{1}{2}s(s-1)$, and so of d_+. Hence $c_+ = d_+$. Writing u for $\frac{1}{2}s(s-1)$, we have

$$d = 2^t d_+ = 1 + u(d_+ - 1) \qquad (2^t = 1 \text{ or } 2;\ 1)\ . \tag{4}$$

Whence, for $2^t = 1$, we have

$$d = d_+\ ,\ (u-1)(d_+ - 1) = 0\ , \tag{5}$$

that is, either the $G^d = G_{d=d_+=1}$ or $u = 1$, $s = 2$; and, for $2^t = 2$, we have

$$d = 2\,d_+\ ,\ (u-2)(d_+ - 1) = 1\ , \tag{6}$$

that is, $d_+ = 2$, $u = 3$, $s = 3$. Hence, as was stated, $d = 1$ or $s = 2$ or 3.

The two remaining groups $G^{s+1}_{M(s)}$ $s = 2, 3$ are in fact composite, being (§ 1) the G^3_6-symmetric and the G^4_{12}-alternating with the respective self-conjugate subgroups G^3_3-cyclic and G^4_4-four-group.

§ 9. SUBGROUPS OF $G_{M(s)}$: THE CYCLIC, THE DIHEDRON, AND THE FOUR-GROUP (WITH CYCLIC BASES NOT OF SET I)

I recall the formulas for the abstract k-dihedron group G_{2k} based on the cyclic G^k:

$$A^k = I,\ B^2 = I,\ AB = BA^{-1}\ , \tag{1}$$

whence

$$BAB^{-1} = A^{-1},\ ABA^{-1} = BA^{-2}\ . \tag{2}$$

Hence under the G_{2k} the operators A^g and A^{-g} are conjugate (g=0, 1, 2, $\cdots$), and the k operators BA^i ($i = 0, 1, \cdots, k-1$) of period two form one set or two sets of conjugate operators according as k is odd or even, and then the cyclic base G_k is self-conjugate and the k cyclic groups G_i form one set or two sets of conjugate subgroups.

A cyclic G_k contains one subgroup G_d for every divisor d of k.

A dihedron G_{2k} contains based on such a cyclic G_d of its cyclic base G_k in all k/d dihedron G_{2d}. These k/d groups G_{2d} form under the G_{2k} one system or two systems of conjugate subgroups according as k/d is odd or even.[19] In the former case the G_{2d} is self-conjugate only under itself. In the latter case the G_{2d} is self-conjugate under a dihedron $G_{2.2d}$.

Cyclic G_k and dihedron G_{2k} contain no subgroups other than those just mentioned.

Now (§6 II, III) *the* $G_{M(s)}$ *contains* $\frac{1}{2}s(s \pm 1)$ conjugate largest cyclic subgroups $G_{\frac{s\mp1}{2;1}}$ of sets $\frac{\text{II}}{\text{III}}$, and hence precisely as many *conjugate cyclic* $G_{d_\mp}$ *where* $d_\mp$ *is any divisor of* $\frac{s\mp1}{2;1}$.

[19] *Cf.* KLEIN-FRICKE, *loc. cit.*, p. 468.

Every cyclic $G_{\frac{s\mp1}{2;1}}$ lies in one dihedron $G_{2\cdot\frac{s\mp1}{2;1}}$; within the $G_{(2;1)M(s)}$ these extend to a cyclic $G_{s\mp1}$ and a dihedron $G_{2(s\mp1)}$.

Every cyclic or dihedron subgroup of the $G_{M(s)}$ with cyclic base not of set I lies in one of these dihedron $G_{2\frac{s\mp1}{2;1}}$.

Every cyclic $G_{d_\mp}$ is the cyclic base of $\frac{s\mp1}{2;1}/d_\mp$ dihedron $G_{2d_\mp}$.

Two dihedron $G_{2d_\mp}$ belonging to the same dihedron $G_{2\frac{s\mp1}{2;1}}$ if conjugate under the $G_{M(s)}$ are conjugate[20] under the $G_{2\cdot\frac{s\mp1}{2;1}}$. Under the $G_{2\cdot\frac{s\mp1}{2;1}}$ the $\frac{s\mp1}{2;1}/d_\mp$ $G_{2d_\mp}$ form one system or two systems of conjugate groups according as $\frac{s\mp1}{2;1}/d_\mp$ is odd or even; within the dihedron $G_{2(s\mp1)}$ of the $G_{(2;1)M(s)}$ they form one system of conjugate groups.

Every dihedron $G_{2d_\mp}$ $(d_\mp>2)$ contains only one basal cyclic $G_{d_\mp}$.

There are in the $G_{M(s)}$ in all $M(s)/2d_\mp$ dihedron $G_{2d_\mp}$ $(d_\mp>2)$ which form one system or two systems of conjugate groups according as $\frac{s\mp1}{2;1}/d_\mp$ is odd or even. In the former case a $G_{2d_\mp}$ is self-conjugate only under itself; in the latter case a $G_{2d_\mp}$ is self-conjugate under a dihedron $G_{2\cdot2d_\mp}$. These $G_{2d_\mp}$ within the $G_{(2;1)M(s)}$ form only one system.

The $G_{M(s)}$ always contains operators V_2 of period 2. If $q=2$, then these V_2 all are of set I. If $q>2$, then these V_2 all belong to set II or to set III according as $\frac{1}{2}(s-1)$ or $\frac{1}{2}(s+1)$ is even. Now for $q>2$, $s=q^n$ is of the form $4h+1$ or $4h-1$, according as the Jacobi-Legendre symbol $\left(\frac{-1}{s}\right)$ is $+1$ or -1; hence $\frac{1}{2}\left[s-\left(\frac{-1}{s}\right)\right]$ is even, and all the V_2 belong to the $\frac{1}{2}\left[s+\left(\frac{-1}{s}\right)\right]$ conjugate cyclic $G_{\frac{1}{2}\left[s-\left(\frac{-1}{s}\right)\right]}$ (§6 II, III).

The four-groups $G_4=G_{2d}$ $(d=2)$ with cyclic bases not of set I remain for consideration. The $G_{M(s)}$ $(s=q^n,\ q>2)$ contains (§6 II, III) $\frac{1}{2}s\left[s+\left(\frac{-1}{s}\right)\right]$ conjugate cyclic G_2. Every G_2 lies in $\frac{1}{4}\left[s-\left(\frac{-1}{s}\right)\right]$ four-groups G_4. Every G_4 contains 3 G_2. *There are in the $G_{M(s)}$ $(s=q^n,\ q>2)$ in all $M(s)/12$ four-groups G_4; these form one system or two systems of conjugate groups according as $\frac{1}{4}\left[s-\left(\frac{-1}{s}\right)\right]$ is odd or even,*

[20] [Proof for $d_\mp=2$ (and so $q>2$)]. A four-group G_4 $(d_\mp=2;\ q>2)$ has three substitutions T_1, T_2, T_3 of period 2. Within the $G_{M(s)}$ the G_4 is self-conjugate under a group $G_{4u}\{U\}$. The substitutions U as transformers, I affirm, permute the T's transitively; from this fact the statement of the text follows at once. For otherwise one T, say T_1, would be self-conjugate under the G_{4u}, and so the G_{4u} would be a subgroup (in fact, dihedron) of the dihedron $G_{2\frac{s\mp1}{2}}$ corresponding to T_1 (§ 6, II, III); hence the G_4 would be self-conjugate under exactly itself ($u=1$) or a dihedron G_8 ($u=2$), and so would be within the $G_{M(s)}$ one of a system of $M(s)/4$ or $M(s)/8$ conjugate four-groups; but, as is immediately proved in the text, the $G_{M(s)}$ $(q>2)$ contains in all $M(s)/12$ four-groups.

that is, according as $s = q^n$ *has the form* $8h \pm 3$ or $8h \pm 1$. *In the former case a* G_4 *is self-conjugate under a* G_{12}, *in the latter case under a* G_{24}. *These* G_4 *form within the* $G_{\mathfrak{T}M(s)}$ *only one system; every* G_4 *is self-conjugate under a* G_{24}. These groups G_{12}, G_{24} have the tetrahedron, octahedron type (§§ 13 (4°), 15 (IV, V), 18).

We have now completely enumerated the cyclic, dihedron, and four-group subgroups of the $G_{M(s)}$ whose cyclic bases are not of set I.

Within the $G_{\mathfrak{T}M(s)}$ $(q>2)$ every cyclic $G_{d_\mp}$ $(d_\pm > 1)$ of the cyclic $G_{\frac{s\mp1}{2}}$ of the $G_{M(s)}$ extends to a definite cyclic $G_{\mathfrak{T}d_\mp}$ of the cyclic $G_{s\mp1}$ and every dihedron $G_{\mathfrak{T}.d_\mp}$ of the $G_{M(s)}$ to a definite dihedron $G_{\mathfrak{T}.2d_\mp}$ (which belong to the $G_{M(s)}$ only if $(s\mp1)/2d_\mp$ is even). Conversely, if d is even and >2, every cyclic G_d and dihedron $G_{\mathfrak{T}.d}$ of the $G_{\mathfrak{T}M(s)}$ (with cyclic base not of set I) is the extension of a definite similar group of the $G_{M(s)}$. We find that:

The $G_{\mathfrak{T}M(s)}$ $(q>2)$ *contains for every divisor* $d>2$ *of* $s \pm 1$ *one system of conjugate cyclic* G_d *and one or two systems of conjugate dihedron* $G_{\mathfrak{T}.d}$ *according as* d *is even or odd. The* $G_{\mathfrak{T}M(s)}$ *contains a system of* $\frac{1}{2}s\left[s+\left(\frac{-1}{s}\right)\right]$ *conjugate* $G_\mathfrak{T}'$ *(of the* $G_{M(s)}$*) and another system of* $\frac{1}{2}s\left[s-\left(\frac{-1}{s}\right)\right]$ *conjugate* $G_\mathfrak{T}'$ *(not of the* $G_{M(s)}$*).* The $G_{\mathfrak{T}M(s)}$ *contains a system of* $M(s)/12$ *conjugate four-groups* $G_{\mathfrak{T}.2}'$ *and another system of* $M(s)/4$ *four-groups* $G_{\mathfrak{T}.2}''$; *a* $G_{\mathfrak{T}.2}'$ *contains three* $G_\mathfrak{T}'$, *while a* $G_{\mathfrak{T}.2}''$ *contains one* $G_\mathfrak{T}'$ *and two* $G_\mathfrak{T}''$.

§ 10. SUBGROUPS OF $G_{M(s)}$:

COMMUTATIVE SUBGROUPS OF THE $s+1$ $G_s^{(\kappa)}$ OF SET I (§6, I)

The $s+1$ $G_s^{(\kappa)}$ of set I are conjugate under the $G_{M(s)}$ (§ 6, I). We study the subgroups of $G_s^{(\infty)}$ $\{S_\beta\}$. This is a commutative group of order $s = q^n$; every operator is of period q. To every subgroup G_{q^m} of order q^m $(m \leqq n)$ corresponds an additive-group of rank m in the Galois-field $GF[s = q^n]$, and conversely.

Writing $B(n, m, x)$ for Gauss's cyclotomic function[21] (n, m),

$$B(n,m,x) = \frac{(x^n-1)(x^{n-1}-1)\cdots(x^{n-m+1}-1)}{(x^m-1)(x^{m-1}-1)\cdots(x-1)}, \tag{1}$$

we readily see that there are in the $G_{s=q^n}$ exactly $B(n, m, q)$ subgroups G_{q^m}.

We consider one such subgroup $G = G_{q^m}\{S_\lambda\}$ where λ ranges over an additive-group $[\lambda_1, \cdots, \lambda_m]$ of rank m (§ 2, 19°) and inquire as to the largest group H within the $G_{M(s)}$ under which G is self-conjugate. H must be a subgroup of the $G^{(\infty)}_{\frac{s(s-1)}{2;1}}$ $\{V = (a,0;0,a^{-1})\}$ (§ 6, I). V transforms S_λ into $S_{a^2\lambda}$, and the group $G_{q^m}\{S_\lambda\}$, $\lambda = [\lambda_1, \cdots, \lambda_m]$, into the group $G' = G_{q^m}\{S_{a^2\lambda}\} = G_{q^m}\{S_{\lambda'}\}$, $\lambda' = [a^2\lambda_1, \cdots, a^2\lambda_m]$. Suppose that there are in all e marks $\alpha = \epsilon$ (say $\epsilon_1, \cdots, \epsilon_e$), such that the two

[21] GAUSS, *Werke*, Vol. II, p. 16; GAUSS-MASER, p. 467.

additive-groups $[\lambda_1, \cdots, \lambda_m]$ and $[\epsilon^s\lambda_1, \cdots, \epsilon^s\lambda_m]$ are the same. (The marks $\epsilon = \pm 1$; 1 are such marks ϵ. Hence $e \geqq 2; 1$). Then the $\frac{se}{2;1}$ operators V:

$$V = (\epsilon, \epsilon\beta; 0, \epsilon^{-1}) = (\epsilon^s, 0; 0, 1)\ (1, \beta; 0, 1), \tag{2}$$

where independently β ranges over the $GF[s]$ and ϵ ranges over the e marks $\epsilon_1, \cdots \epsilon_e$, constitute the largest group $H = G_{\frac{se}{2;1}}$ under which $G = G_{q^m}\ \{S_\lambda\}$ is self-conjugate.

The determination for any given group $G = G_{q^m}\{S_\lambda\}$ of the group H has then been made to depend upon the determinations for the additive-group $[\lambda_1, \cdots, \lambda_m]$ of rank m, *first*, say of its *multipliers* κ, that is, of all the marks κ such that

$$[\lambda_1, \cdots, \lambda_m] = [\kappa\lambda_1, \cdots, \kappa\lambda_m]\ , \tag{3}$$

and, *secondly*, of all the marks ϵ whose squares are multipliers.

It turns out (§11) that the multipliers κ are the marks κ $(\kappa \neq 0)$ of (a definite so-called) the multiplier Galois-field $GF\ [q^k]$ of the additive-group $[\lambda_1, \cdots \lambda_m]$. We discriminate the cases

$$(q > 2)\ n/k \text{ even},\ n/k \text{ odd};\ (q = 2)\ . \tag{4}$$

Then (§ 2, 50°, 39°) there are

$$e = (2, 1; 1)\ (q^k - 1) \tag{5}$$

marks ϵ, and the group $G = G_{q^m}\{S_\lambda\}$ is within the $G_{M(s)}$ or the $G^{(\infty)}_{\frac{s(s^k-1)}{2;1}}$ self-conjugate under the group H (2) of order

$$\frac{se}{2;1} = \frac{s(q^k-1)}{1, 2; 1}\ , \tag{6}$$

and so is one of a system of

$$\frac{(s+1)(q^n-1)}{(2, 1; 1)(q^k-1)} \text{ or } \frac{q^n-1}{(2, 1; 1)(q^k-1)} \tag{7}$$

conjugate groups.

Within the $G_{2M(s)}(q > 2)$ the subgroups $G_{q^m}\{S_\lambda\}$ of the type of § 10 are precisely those of the $G_{M(s)}$. However, the systems of conjugate groups of the $G_{M(s)}$ with odd n/k (4) unite by pairs to form the systems of conjugate groups of the $G_{2M(s)}$, for the two $G_{q^m}\{S_\lambda\}$ with $\lambda = [\lambda_1', \cdots, \lambda_m']$ and $\lambda = [\rho'\lambda_1', \cdots, \rho'\lambda_m']$, where ρ' is a primitive root of the multiplier $GF[q^k]$ of the additive-group $[\lambda_1', \cdots, \lambda_m']$, are conjugate in the $G_{2M(s)}$ but not in the $G_{M(s)}$.—The group $G_{q^m}\{S_\lambda\}$ is within the $G_{(2;1)M(s)}$ self-conjugate under the group $H'_{q^n(q^k-1)}$ of substitutions $D_\kappa S_\beta$ $(\kappa \neq 0)$

$$(\kappa, \kappa\beta; 0, 1) = (\kappa, 0; 0, 1)\ (1, \beta; 0, 1). \tag{8}$$

§11. ADDITIVE-GROUPS IN THE GALOIS-FIELD $GF[q^n]$ AND THEIR CORRESPONDING MULTIPLIER GALOIS-FIELDS

In the $GF[s = q^n]$ the additive-group $[\lambda_1, \cdots, \lambda_m]$ of rank m $(m \leqq n)$ based upon the m marks λ_i linearly independent with respect to the $GF[q]$ contains (§ 2, 19°) the q^m distinct marks λ of the form

$$\lambda = c_1\lambda_1 + \cdots + c_m\lambda_m \tag{1}$$

where the c_i's are integral marks.

If the q^m marks λ are multiplied by any particular mark μ ($\mu \neq 0$) then the resulting q^m marks $\mu\lambda$ constitute the additive-group $[\mu\lambda_1, \cdots, \mu\lambda_m]$ or $\mu[\lambda_1, \cdots, \lambda_m]$ likewise of rank m. We may say that $[\mu\lambda_1, \cdots, \mu\lambda_m]$ is derived from $[\lambda_1, \cdots, \lambda_m]$ by multiplication by μ.

We seek (§10, (3)) the multipliers $\mu = \kappa$ of the $[\lambda_1, \cdots, \lambda_m]$, that is, those multipliers $\mu = \kappa$ under multiplication by which $[\lambda_1, \cdots, \lambda_m]$ is invariant. These multipliers κ constitute obviously a multiplicative-group. Further, together with the mark 0, they constitute an additive-group with respect to the field $GF[q]$ of integral marks. For, if κ_1 and κ_2 are any two multipliers κ then under multiplication by $\mu = \kappa_1 + \kappa_2$ the $[\lambda_1, \cdots, \lambda_m]$ becomes $[\mu\lambda_1, \cdots, \mu\lambda_m]$ which is an additive-group, on the one hand, included within the $[\lambda_1, \cdots, \lambda_m]$ and, on the other hand, unless $\mu = 0$, of rank m. Hence, the mark $\mu(\mu = \kappa_1 + \kappa_2)$ is either 0 or a multiplier κ.

The marks 0 and the multipliers κ constitute then a Galois-field $GF[q^k]$ of rank k included within the fundamental $GF[q^n]$. We call this $GF[q^k]$ THE *multiplier Galois-field*, and every $GF[q^{k'}]$ included within it A *multiplier Galois-field* of the additive-group $[\lambda_1, \cdots, \lambda_m]$ of rank m, and the integer k its *multiplicative-index*. k' is a divisor of k, and k is a divisor of n (§2, 39°) and indeed (as we shall prove in a moment) also of m. There are $q^k - 1$ multipliers κ.

The multiplier $GF[q^k]$ of the additive-group $[\lambda_1, \cdots, \lambda_m]$ is the (largest) additive-group common to the m additive-groups

$$[\lambda_i^{-1}\lambda_1, \cdots, \lambda_i^{-1}\lambda_m] \qquad (i = 1, 2, \cdots, m), \tag{2}$$

and it is, moreover, contained in the $q^m - 1$ additive-groups

$$[\lambda^{-1}\lambda_1, \cdots, \lambda^{-1}\lambda_m] \qquad (\lambda \text{ of } [\lambda_1, \cdots, \lambda_m], \lambda \neq 0). \tag{3}$$

The additive-group $[\lambda_1, \cdots, \lambda_m]$ of rank m with respect to the $GF[q]$ may with respect to any such multiplier $GF[q^{k'}]$ be exhibited as an additive-group $[\lambda_1', \cdots, \lambda_{m/k'}' \mid GF[q^{k'}]]$ of rank m/k' (§2, 24°). Hence, every such k' is a divisor of m, and the multiplicative-index k is itself such a k'.

Conversely, every additive-group with respect to any $GF[q^k]$ has that $GF[q^k]$ as *a* multiplier $GF[q^k]$.

With respect to any four positive integers q (a prime), n, m, k, we introduce the arithmetic-functional notations

$$A(q, n, m, k), \quad A[q, n, m, k] \tag{3}$$

to designate the number within a $GF[q^n]$ of additive-groups of rank m having the included $GF[q^k]$ as respectively *a*, *the* multiplier $GF[q^k]$. We set at once

$$A(q, n, m, k) = A[q, n, m, k] = 0, \tag{4}$$

unless the q, n, m, k satisfy the conditions:

$$q \text{ a prime}, \; n \geqq m, \; k \text{ a common divisor of } n \text{ and } m. \tag{5}$$

Attending then only to cases (5) we introduce the integers h, l, u, and v, so that

$$[m, n] = l = hk, \; m = lu = hkv, \; n = lv = hkv, \; [u, v] = 1, \; u \leqq v. \tag{6}$$

Then we find easily

$$A(q,n,m,k)=\frac{(q^n-1)(q^n-q^k)(q^n-q^{2k})\cdots(q^n-q^{(hu-1)k})}{(q^m-1)(q^m-q^k)(q^m-q^{2k})\cdots(q^m-q^{(hu-1)k})}\ . \tag{7}$$

We recall the cyclotomic function (λ, μ) of Gauss with its more explicit notation $B(\lambda, \mu, x)$ of §10 (1). In this notation we have

$$A(q,n,m,k)=B(hv,hu,q^k)=B(n/k,m/k,q^k)\ . \tag{8}$$

For fixed q, n, and m, and so for fixed l, u, and v we write, for variable k and h, complementary divisors of l, $(l=hk)$,

$$A(q,n,m,k)=B(h),\quad A[q,n,m,k]=B[h],\quad [m,n]=l=hk. \tag{9}$$

The functions $B(h)$, $B[h]$ are well-defined, single-valued arithmetic functions of the argument h for all positive integers h *which are divisors of* $l=[m,n]$.

We have obviously

$$B(h)=\sum_{d\mid h} B[d]\ , \tag{10}$$

where the summation-remark $d \mid h$ denotes that d runs over the divisors of h. Hence, introducing Kronecker's[22] symbols δ_{ij} and ϵ_t for all numbers i, j and for all positive integers t,

$$\delta_{ij}=\begin{cases}1\ , & \text{if } i=j,\\ 0\ , & \text{if } i\neq j;\end{cases} \tag{11}$$

$$\epsilon_t=\begin{cases}1\ , & \text{if } t \text{ is } 1,\\ 0\ , & \text{if } t \text{ is divisible by the square of any prime,}\\ (-1)^r, & \text{if } t \text{ is the product of } r \text{ distinct primes,}\end{cases} \tag{12}$$

and noticing that

$$\sum_{d\mid t}\epsilon_d=\delta_{1t}\ , \tag{13}$$

we find[22, 23] that

$$B[h]=\sum_{\substack{d\mid h\\ dd'=h}}\epsilon_d\ B(d')\ . \tag{14}$$

From (9, 6, 14, 8) we have the determination

$$A[q,n,m,k]=\sum_{d\mid h}\epsilon_d A(q,n,m,kd)=\sum_{d\mid h}\epsilon_d B(n/kd,m/kd,q^{kd}) \qquad ([m,n]=l=hk). \tag{15}$$

We are thus led to associate with Gauss's function $B(hv, hu, x)$, where h, u, v are positive integers, $v \geqq u$, and $[u, v]=1$, the (so far as I know) new cyclotomic function $B[hv, hu, x]$, so that

$$B[hv,hu,x]=\sum_{d\mid h}\epsilon_d B(hv/d,hu/d,x^d)\ , \tag{16}$$

$$B(hv,hu,x)=\sum_{d\mid h} B[hv/d,hu/d,x^d]\ . \tag{17}$$

The functions $B(hv, hu, x)$, $B[hv, hu, x]$ are rational integral functions of x with rational integral coefficients. Further $B[hv, hu, 0]=\delta_{1h}$, and it may be shown that $B[hv, hu, x]$ has the factor $x^{1-\delta_{1h}}(x^{hv}-1)/(x-1)$.

[22] *Cf.* KRONECKER, *Berliner Sitzungsberichte*, July 29, 1886, p. 708, and April 5, 1888, p. 418.

[23] DIRICHLET-DEDEKIND, *Zahlentheorie*, 4th ed., supp. VII, *Über einige Sätze aus der Theorie der Kreistheilung*, pp. 360-70.

We have, then, in the notations of § 10 (1), § 11 (3, 5, 6), from (8, 15),

$$A(q, n, m, k) = B(hv, hu, q^k) \ , \tag{18}$$

$$A[q, n, m, k] = B[hv, hu, q^k] \ . \tag{19}$$

§ 12. SUBGROUPS OF $G_{M(\theta)}$: NON-COMMUTATIVE SUBGROUPS OF THE $s+1$ $G^{(\kappa)}_{\frac{s(s-1)}{2;1}}$ (§ 6, I)

(1°) The $s+1$ $G^{(\kappa)}_{\frac{s(s-1)}{2;1}}$ are conjugate under the $G_{M(\theta)}$ (§ 6, I). We study the $G^{(\infty)}_{\frac{s(s-1)}{2;1}}\{(\alpha, \beta; 0, \alpha^{-1})\}$. This is made up (§ 6 I, II) of the $G^{(\infty)}_s\{S_\beta\}$ as self-conjugate subgroup and the s conjugate groups $G^{(\infty\mu)}_{\frac{s-1}{2;1}}$ $(\mu \neq \infty)$. We make the ordinary matricular arrangement of the substitutions of $G^{(\infty)}_{\frac{s(s-1)}{2;1}}$ with respect to the (self-conjugate) subgroup $G^{(\infty)}_s$; we may take the substitutions of the cyclic $G^{(\infty 0)}_{\frac{s-1}{2;1}}$ as the extending substitutions; hence the (abstract) quotient-group $G^{(\infty)}_{\frac{s(s-1)}{2;1}}/G^{(\infty)}_s$ is the (abstract) cyclic $G_{\frac{s-1}{2;1}}$; its only subgroups are the cyclic G_{d_-} for every d_- divisor of $\frac{s-1}{2;1}$.

Every subgroup G^* of the $G^{(\infty)}_{\frac{s(s-1)}{2;1}}$ has its substitutions lying on the face of that matricular arrangement in such a way as to exhibit their matricular arrangement with respect to the subgroup $G = G_{q^m}\{S_\lambda\}$, $\lambda = [\lambda_1, \cdots, \lambda_m]$, of its substitutions of period q (§ 10). This is a self-conjugate subgroup. The quotient-group G^*/G_{q^m} must be such a cyclic G_{d_-}. A substitution V in that line of the G^*-arrangement which corresponds to the generator of the quotient cyclic G_{d_-} has itself the period d_-, for V^{d_-} lies in the group G_{q^m}.

The s groups $G^{(\infty\mu)}_{\frac{s-1}{2;1}}$ are conjugate (§ 6, II) under the transformers S_β, which transform $G_{q^m}\{S_\lambda\}$ into itself.

We obtain a representative under $G^{(\infty)}_{\frac{s(s-1)}{2;1}}$ of every G^* based on a particular $G_{q^m}\{S_\lambda\}$ when we extend the $G_{q^m}\{S_\lambda\}$ by the various cyclic $G^{(\infty 0)}_{d_-}$ under which it is self-conjugate.

Now the $G_{q^m}\{S_\lambda\}$ is self-conjugate under the group $H_{\frac{s(q^k-1)}{1,2;1}}$ (§ 10 (2, 4, 5, 6)) obtained by extending the $G^{(\infty)}_s$ by the cyclic $G^{(\infty 0)}_{\frac{q^k-1}{1,2;1}}$. Our representative $G^*_{q^m d_-}$ is obtained by extending the $G_{q^m}\{S_\lambda\}$ by a cyclic $G^{(\infty 0)}_{d_-}$ subgroup of this $G^{(\infty 0)}_{\frac{q^k-1}{1,2;1}}$. The $G^*_{q^m d_-}$ is made up of the $G_{q^m}\{S_\lambda\}$ and q^m cyclic $G^{(\infty\lambda)}_{d_-}$; it is self-conjugate under the $G_{\frac{q^m(q^k-1)}{1,2;1}}$ obtained by extending the $G_{q^m}\{S_\lambda\}$ by the $G^{(\infty 0)}_{\frac{q^k-1}{1,2;1}}$, and so is one of a system of $(q^n+1)\,q^{n-m}\,(q^n-1)/(2,1;1)\,(q^k-1)$ conjugate groups.

A subgroup G^* of $G^{(\infty)}_{\frac{s(s-1)}{2;1}}$ which contains no substitution of period q is a cyclic subgroup $G^{(\infty\mu)}_{d_-}$ of one of the cyclic $G^{(\infty\mu)}_{\frac{s-1}{2;1}}$. This remark is of importance in the theory of those subgroups of the $G_{M(\theta)}$ which contain no operators of period q.

(2°) The typical non-commutative subgroup of the $G^{(\infty)}_{s(s-1)}$ of the $G_{(2;1)M(s)}$ is the $G^{*}_{q^m d_-}$ obtained by extending the general $G_{q^m}\{S_\lambda\}$ of § 10 by a cyclic $G^{(\infty 0)}_{d_-}$ subgroup of the $G^{(\infty 0)}_{q^k-1}\{D_\kappa\}$ $(\kappa \neq 0)$ (§ 10 (8)). This $G^{*}_{q^m d_-}$ is self-conjugate under the $G^{*}_{q^m(q^k-1)}\{D_\kappa S_\lambda\}$, and thus determines a system of

$$(q^n+1)\,q^{n-m}\,(q^n-1)/(q^k-1)$$

conjugate subgroups.

(3°) The $G^{(\infty)}_{s(s-1)}$ contains no octahedron or icosahedron subgroups, and tetrahedron subgroups only in case $q=2$, $n=$ even, $m=k=2$, $e=3$. In this case the $G_{(2;1)M(s)}=G_{M(s)}$ $(q=2)$ contains $M(s)/12$ tetrahedron groups, all conjugate with the group $G^{(\infty)}_{4.3=12}(\alpha,\beta;0,1)$, where α $(\alpha\neq 0)$ and β are marks of the $GF[2^2]$. (*Cf.* §15, 2°.)

§ 13. SUBGROUPS OF $G_{M(s)}$ CONTAINING OPERATORS OF PERIOD q

(1°) The substitutions of period q, hence of set I, of the (any) subgroup G_Ω of the $G^{s+1}_{M(s)}$ distribute themselves over certain $s+1$ subgroups $G^{(\mu)}_{q^{m_\mu}}$ of the $s+1$ groups $G^{(\mu)}_{s}$ (§ 10). Of the $s+1$ orders q^{m_μ} at least one is by hypothesis greater than 1. By suitable transformation within the $G_{M(s)}$ we arrange it so that $q^{m_\infty}>1$, $m=m_\infty>0$. Under the q^m transformers S_β of the $G^{(\infty)}_{q^m}$ the remaining $G^{(\mu)}_{q^{m_\mu}}$ with $m_\mu>0$ $(\mu\neq\infty)$ (if any) arrange themselves in sets, each consisting of q^m conjugate groups. Under the G_Ω the $G^{(\infty)}_{q^m}$ is then one of a set of $1+fq^m$ conjugate groups, where f is a positive or zero integer. The G_Ω contains no group $G^{(\mu)}_{q^{m_\mu}}$ $(m_\mu>0)$ other than the $1+fq^m$ groups of this set. For any such group $G^{(\mu)}_{q^{m_\mu}}$ would be one of a set of n_μ conjugate groups, where n_μ would necessarily have at the same time the forms (by parity of reasoning) $n_\mu=1+f_\mu q^{m_\mu}$ and (by the previous considerations) $n_\mu=f'_\mu q^m$.

Every G_Ω which contains operators of period q contains these operators in $1+fq^m$ groups $G^{(\mu)}_{q^m}$ conjugate under the G_Ω, where for each group G_Ω f and m are properly determined integers $f\geqq 0, m>0$.

The groups G_Ω with $f=0$ we have already enumerated (§§ 10, 12), since every such group lies in a group $G^{(\mu)}_{\frac{s(s-1)}{2;1}}$ (§ 6, I).

(2°) We proceed to the general group G_Ω with $f\geqq 1$ and with $m=m_*>0$. It contains $1+fq^m$ groups $G^{(\mu)}_{q^m}$ conjugate with a certain group $G^{(\infty)}_{q^m}=G_{q^m}\{S_\lambda\}$, $\lambda=[\lambda_1,\cdots,\lambda_m]$. This $G^{(\infty)}_{q^m}$ is within the G_Ω self-conjugate under a certain $G^{(\infty)}_{q^m d_-}$ (§12), and hence

$$\Omega=(1+fq^m)\,q^m d_- \,. \tag{1}$$

By transformation[24] by a substitution of the $G^{(\infty)}_{\frac{s(s-1)}{2;1}}$ suitably chosen we arrange it so that this $G^{(\infty)}_{q^m d_-}$ is

$$G^{(\infty)}_{q^m d_-}\{V_{\eta,\lambda}\}\,,\quad V_{\eta,\lambda}=\left(\frac{\eta,\eta\lambda}{0,\eta^{-1}}\right)=\left(\frac{\eta,0}{0,\eta^{-1}}\right)\left(\frac{1,\lambda}{0,1}\right)=P_\eta S_\lambda\,, \tag{2}$$

[24] If $d_-=1$, this transformation is not needed here and remains available for other purposes.

obtained by extending the $G^{(\infty)}_{q^m}\{S_\lambda\}$ by the cyclic $G^{(\infty\,0)}_{d_-}\{P_\eta\}$ contained within the cyclic $G^{(\infty\,0)}_{\frac{e}{2;1}}\{P_\epsilon\}$. There are $(2;1)\,d_-$ marks η, the distinct powers of a mark η_0; in particular, $\eta_0^{d_-} = -1$. Of course, $P_\eta = P_{-\eta}$, $V_{\eta,\lambda}, = V_{-\eta,\lambda}$.

Now (§§ 10, 11) the squares of the marks η (*quâ* marks ϵ) are multipliers κ of the $[\lambda_1, \cdots, \lambda_m]$. The multiplier $GF[q^k]$ lies in $[\lambda_0^{-1}\lambda_1, \cdots, \lambda_0^{-1}\lambda_m]$ where λ_0 is any mark $\lambda \neq 0$ (§ 11 (3)). We have

$$P_\sigma(\alpha, \beta; \gamma, \delta)\,P_\sigma^{-1} = (\alpha, \sigma^2\beta; \sigma^{-2}\gamma, \delta), \quad P_\sigma\,V_{\eta,\lambda}\,P_\sigma^{-1} = V_{\eta,\sigma^2\lambda}\,. \tag{3}$$

Hence, by transformation of $G_{M(\omega)}$ and G_Ω by $P_{\sqrt{\lambda_0^{-1}}} = D_{\lambda_0^{-1}}$ $(\omega' = \lambda_0^{-1}\omega)$ of the $G_{(2;1)\,M(\omega)}$ (§ 4) we have $G_{M(\omega)}$ and within it G^*_Ω whose additive-group $[\lambda_1^*, \cdots, \lambda_m^*]$ contains the mark $\lambda^* = 1$ and so the marks of its multiplier $GF[q^k]$. We suppose that this transformation has been made; we drop the $*$'s.

(3°) The G_Ω of order $\Omega = (1 + fq^m)\,q^m d_-$ is obtained by extending the $G^{(\infty)}_{q^m d_-}\{V_{\eta,\lambda}\}$ by the identity and certain fq^m extenders V_j $(j = 1, \ldots, fq^m)$,

$$V_j = \left(\frac{\alpha_j, \beta_j}{\gamma_j, \delta_j}\right), \quad V_j\,V_{\eta,\lambda} = \left(\frac{\alpha_j\eta\,,\ \alpha_j\eta\lambda + \beta_j\eta^{-1}}{\gamma_j\eta\,,\ \gamma_j\eta\lambda + \delta_j\eta^{-1}}\right) \qquad (\gamma_j \neq 0;\ j = 1, \ldots, fq^m)\,. \tag{4}$$

The G_Ω contains $(1 + fq^m)\,(q^m - 1)$ substitutions of set I. Of these $q^m - 1$ are in the $G^{(\infty)}_{q^m}\{S_\lambda\}$. The remaining $fq^m(q^m - 1)$ are substitutions $V_j\,V_{\eta,\lambda}$ satisfying the necessary and sufficient condition (§ 6, V(I)):

$$\alpha_j\eta + \delta_j\eta^{-1} + \gamma_j\eta\lambda = \pm 2\,. \tag{5}$$

For given V_j and η $(\gamma_j \neq 0,\ \eta \neq 0)$ there are at most 2; 1 values of λ satisfying (5). For given V_j $(\gamma_j \neq 0)$ there are at most $(2;1)d_-$ substitutions $V_{\eta,\lambda}$ $(V_{\eta,\lambda} = V_{-\eta,\lambda})$ such that $V_j\,V_{\eta,\lambda}$ is of set I. Hence by §§ 10, 11, 12

$$q^m - 1 \leqq (2;\ 1)\,d_- \leqq e = (2,\ 1;\ 1)\,(q^k - 1) \leqq (2,\ 1;\ 1)\,(q^m - 1)\,. \tag{6}$$

There are in all two cases:

[A] $m = k$, $q^k - 1 = (2;\ 1)\,d_-$, $\Omega = (1 + fq^k)\,q^k\,(q^k - 1)\,/\,(2;\ 1)$.

[B] $m = k$, $q > 2$, $n/k =$ even, $q^k - 1 = d_-$, $\Omega = (1 + fq^k)\,q^k\,(q^k - 1)$.

In each case $m = k$ and so (2°) the additive-group $[\lambda_1, \cdots, \lambda_m]$ is its own multiplier $GF[q^k]$ and every λ is 0 or a multiplier κ.

(4°) [Case A.] $q^k - 1 = (2;1)d_-$ and the η's are the κ's. The equation (5) with V_j and η (or κ) given has exactly 2; 1 solutions λ. We may replace V_j by a $V_j\,V_{\kappa,\lambda}$ of set I. We set then $\delta_j = 2 - \alpha_j$, $\eta = \kappa$, and determine by the equation

$$\alpha_j(\kappa - \kappa^{-1}) + \gamma_j\lambda_{j,\kappa,\pm} = \pm 2 - 2\kappa^{-1} \tag{7}$$

for every j and κ and sign $\pm$ a mark λ, viz., $\lambda_{j,\kappa,\pm}$—a mark $\eta\lambda$ being a mark λ.

Theorem: The G_Ω *is*[25] *the group* $G_{M(q^k)}$ *of* $\Omega = M(q^k) = (1 + q^k)\,q^k\,(q^k - 1)/(2;1)$ *substitutions*

$$V = (\lambda_1,\ \lambda_2;\ \lambda_3,\ \lambda_4) \qquad (\lambda_1\lambda_4 - \lambda_2\lambda_3 = 1) \tag{8}$$

where the $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ *belong to the* $GF[q^k]$.

[25] It appears below, however, that for $q^k = 2^4$ there are other groups G_Ω. For $q^k = 3,\ 5,\ 2^2$ the $G_{M(q^k)}$ is of type tetrahedron, icosahedron, icosahedron (§ 1).

We shall prove that every a_j, β_j, γ_j, δ_j is a λ. Hence G_Ω is a subgroup of the $G_{M(q^k)}$ (8). But we already have $\Omega \geqq M(q^k)$. Hence $f=1$ and $\Omega = M(q^k)$ and $G_\Omega = G_{M(q^k)}$.

[Case $A_{q>2}$.] From (7) for $\kappa=1$ we have $\gamma_j \lambda_{j,1,-} = -4 \neq 0$; hence γ_j is a κ, $\gamma_j = \kappa_j$. Unless $q^k = 3^1$, κ has a value $\kappa \neq \pm 1$, and for such a κ we see from (7) that a_j is a λ, $a_j = \lambda_j$. Also in case $q^k = 3^1$ we have[26] $a_j = \lambda_j$. Hence in every case $\delta_j = 2 - a_j$ is a λ and since $a_j \delta_j - \beta_j \gamma_j = 1$ so is also β_j a λ.

[Case $A^{k\geq 1}_{q=2}$.] κ has a value $\kappa \neq 1$ $(+1 = -1)$ and for such a κ we see from $(7)_{q=2}$ that a_j / γ_j is a λ, say $a_j / \gamma_j = \lambda_j$. Since $q=2$, $\delta_j = a_j$ and $\delta_j / \gamma_j = \lambda_j$. The substitutions $V = V_j \, V_{\kappa,\lambda}$ with j fixed have $a/\gamma = \lambda_j$. If two substitutions $V_{(1)} = V_{j_1} \, V_{\kappa_1, \lambda_1}$ and $V_{(2)} = V_{j_2} \, V_{\kappa_2, \lambda_2}$ have $\lambda_{j_1} = \lambda_{j_2}$, then $j_1 = j_2$. There are fq^k substitutions V_j; $fq^k > 2$. Setting $V_{j_1} \, V_{j_2} = V_{j_3} \, V_{k,\lambda}$, where $j_1 \neq j_2$ and so $\lambda_{j_1} \neq \lambda_{j_2}$, $\lambda_{j_1} + \lambda_{j_2} \neq 0$, we find

$$\lambda_{j_3} = \frac{\lambda_{j_1} \lambda_{j_2}}{\lambda_{j_1} + \lambda_{j_2}} + \frac{1}{\lambda_{j_1} + \lambda_{j_2}} \frac{\beta_{j_1}}{\gamma_{j_1}} \quad .$$

Hence every β_j / γ_j is a λ, $\beta_j / \gamma_j = \lambda'_j$. Since $a_j \delta_j - \beta_j \gamma_j = 1$, $\gamma_j^2 (\lambda_j^2 - \lambda'_j) = 1$, and so γ_j^2 is a λ and hence (since $q=2$) so is γ_j a λ and with γ_j also a_j, δ_j, β_j.

Theorem: The group G_Ω $(q^k = 2^1)$ is a dihedron group G_Ω whose order is $\Omega = 2\,(1+2f)$ (§ 9).

[Case $A^{k=1}_{q=2}$.] The group G_Ω $(q^k = 2^1)$ of order $2(1+2f)$ is obtained by extending $G_2^{(\infty)}$ $\{S_\lambda\}$, where $\lambda = [1] = 0, 1$, by certain $2f$ substitutions V_j of period 2 $(j = 1, \cdots, 2f)$. The $1+2f$ substitutions V_j $(j = 0, \cdots, 2f)$ $(V_0 = S_1)$ form one conjugate set under the G_Ω. Setting $U_j = V_j V_0$, so that $V_j = U_j V_0$, we have $I = V_j^2 = U_j V_0 U_j V_0 = U_j V_0 U_j V_0^{-1}$, so that $V_0 U_j V_0^{-1} = U_j^{-1}$ $(j = 0, \cdots, 2f)$. A substitution U transforms under G_Ω to a U. Hence for V_0 we may substitute $V_{j'}$ and have $I = U_j V_{j'} U_j V_{j'}$. Hence $U_j V_{j'} = U_j U_{j'} V_0$ is of period 2 and so is a $V_{j''} = U_j V_0$. Hence $U_j U_{j'} = U_{j''}$. *The substitutions U_j form a group $G_{\frac{1}{2}\Omega}$.* We have $U_j U_{j'} = (U_{j'}^{-1} U_j^{-1})^{-1} = (U_{j''})^{-1} = V_0 \, (U_{j''}) \, V_0^{-1} = V_0 \, (U_{j'}^{-1} U_j^{-1}) \, V_0^{-1} = (V_0 U_{j'}^{-1} V_0^{-1}) \, (V_0 U_j^{-1} V_0^{-1}) = U_{j'} U_j$. *The group $G_{\frac{1}{2}\Omega} = G_{1+2f}$ is commutative and of odd order. Hence in our case* (§ 6 II, III) *it is cyclic.* Since $V_0 U_j V_0^{-1} = U_j^{-1}$, the group G_Ω is a dihedron $G_{2(1+2f)}$ based on a cyclic G_{1+2f} of set II or III. This dihedron group G_Ω was exhibited in § 9. We obtain as a particular case (for $f=1$) of the dihedron $G_{2(1+2f)}$ the $G_{M(3)}$ called for by the preceding theorem.

(5°) [Case *B.*] $q > 2$, $n/k =$ even. $\Omega = (1+fq^k)\, q^k \, (q^k - 1)$. $q^k - 1 = d_-$.

[26] Case *A:* $q^k = 3^1$, $d_- = 1$. $\lambda = 0, +1, -1$. $\kappa = \eta = \gamma_j = 1, -1$. We may and do restrict η and the γ_j to the value 1.

$V_j \; V_{\eta,\lambda} = V_j S_\lambda$ has as its $a+\delta$ the mark $a_j + \delta_j + \lambda$. For $\lambda = 0, +1, -1$ two of the three values $a_j + \delta_j + \lambda$ are $+2, -2$. Hence $a_j + \delta_j + \lambda$ has the values $0, +1, -1$. By convenient initial choice of the V_j we have $a_j + \delta_j = 0$. The general extender $V_j = V_{(a)}$ is then

$$V_{(a)} = \begin{pmatrix} a, & -1-a^2 \\ 1, & -a \end{pmatrix} .$$

Every substitution of the group $G_\Omega = G_{3(1+2f)}$ has its γ a λ and its $a+\delta$ a λ. Further, by transformation by S_{-a_0}, (*cf.* (2*) above), where a_0 is any particular a, since $S_{-a_0} V_{(a)} S_{-a_0}^{-1} = V_{(a-a_0)}$, we arrange it so that one a is $a = 0$.

$$V_{(0)} = \begin{pmatrix} 0, & -1 \\ 1, & 0 \end{pmatrix} , \quad V_{(0)} \; V_{(a)} = \begin{pmatrix} -1, & -a \\ a, & -1-a^2 \end{pmatrix} .$$

Hence every a *qua* the γ of $V_{(0)} \; V_{(a)}$ is a λ.

The $2d_-$ marks η are the square roots of the q^k-1 marks κ, that is, they are the distinct powers of $\eta_0 = \sqrt{\kappa_0}$, where κ_0 is a primitive root of the Galois-field $GF[q^k]$. In particular there is a mark $\eta = \sqrt{-1}$.

We analyze the G_Ω of this case B with respect to its substitutions T of period 2 (of set II).

The G_Ω contains the $G^{(\infty)}_{q^k(q^k-1)}$ as one of a system of $1+fq^k$ conjugate groups; in $G^{(\infty)}_{q^k(q^k-1)}$ there are q^k conjugate cyclic $G^{(\infty\lambda)}_{q^k-1=d_-}$, and so in all q^k substitutions T, and these are all conjugate with

$$T_0 = (\sqrt{-1}, 0;\ 0, -\sqrt{-1}) \ . \tag{9}$$

Under the G_Ω T_0 is one of a system of $(1+fq^k)\ q^k$ or $\frac{1}{2}(1+fq^k)\ q^k$ conjugate substitutions T according as T_0 is within G_Ω self-conjugate under the cyclic $G^{(\infty 0)}_{q^k-1}$ or under a dihedron $G_{2(q^k-1)}$ obtained by extending it by a substitution T_0' interchanging ∞ and 0 (§ 6 II, § 9). There are then amongst the substitutions $V_j V_{\eta,\lambda}\ (j>0)$ at least fq^{2k} or $\frac{1}{2}(fq^k-1)\ q^k$ substitutions $T = V_j V_{\eta,\lambda}$ satisfying the necessary and sufficient condition (§ 6 end)

$$a_j \eta + \delta_j \eta^{-1} + \gamma_j \eta\lambda = 0 \ . \tag{10}$$

But there are at most $fq^k(q^k-1)$ such substitutions $V_j V_{\eta,\lambda}$. Hence the latter alternative holds; the G_Ω contains a substitution

$$T_0' = (0, -\tau^{-1};\ \tau, 0) \ , \tag{11}$$

and f is odd (since $\frac{1}{2}(fq^k-1)\ q^k$ is an integer).

In case a $V_j\ (j>0)$ gives rise to one or more substitutions $T = V_j V_{\eta,\lambda}$ we replace it by one such T. For these $V_j = T_j$ then we set $\delta_j = -a_j$, and further $\gamma_j = 1$. We attend for the moment only to these V_j's. The substitutions $V_j V_{\eta,\lambda}$ derived from such V_j have $a/\gamma = a_j/\gamma_j$ as a characteristic invariant. The equation $T = V_j V_{\eta,\lambda}$ has always one solution: $V_{\eta,\lambda} = I$, $T = V_j$. If it has two solutions, then the invariant a_j/γ_j is a λ, $a_j/\gamma_j = \lambda_j$. Conversely, whenever $a_j/\gamma_j = \lambda_j$, then the equation has exactly $q^k - 1$ solutions.

By comparing the minimum and maximum numbers for the $T = V_j V_{\eta,\lambda}\ (j>0)$ in the G_Ω we have

$$\tfrac{1}{2}(fq^k-1)\ q^k \leqq q^k(q^k-1) + (f-1)q^k \ . \tag{12}$$

There are in all two cases, $f=1, f=3$:

$[B_{f=1}]$ $q>2$, $n/k =$ even, $\Omega = (q^k+1)\ q^k\ (q^k-1) = 2M\ (q^k)$.

$[B_{f=3}]$ $q=3$, $k=1$, $n =$ even, $\Omega = 60$.

[Case $B_{f=1}$] *Theorem: The group G_Ω is the group*[21] $G_{2M(q^k)}$ *of* $\Omega = 2M(q^k) = (q^k+1)\ q^k\ (q^k-1)$ *substitutions*

$$V = (\lambda_1, \lambda_2;\ \lambda_3, \lambda_4) \qquad (\lambda_1\lambda_4 - \lambda_2\lambda_3 \neq 0) \tag{13}$$

where the $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ *belong to the* $GF[q^k]$ *of which* $\eta_0^2 = \kappa_0$ *is a primitive root. The*

[21] For $q=3$ the group $G_{2M(q^k)}$ is of octahedron type (§ 1).

group $G_{2M(q^k)}$ is obtained by extending its self-conjugate subgroup $G_{M(q^k)}\{V\}$ of substitutions V of square determinant by P_{η_0},

$$P_{\eta_0}=(\eta_0, 0;\ 0, \eta_0^{-1})=(\kappa_0, 0;\ 0, 1)=D_{\kappa_0}\ . \tag{14}$$

We have in the T_λ',

$$T_\lambda'=S_\lambda\ T_0'\ S_{-\lambda}=\left(\frac{1,\lambda}{0,1}\right)\left(\frac{0,-\tau^{-1}}{\tau,0}\right)\left(\frac{1,-\lambda}{0,1}\right)=\left(\frac{\lambda\tau,-\lambda^2\tau-\tau^{-1}}{\tau,-\lambda\tau}\right)\ , \tag{15}$$

$q^k=fq^k$ substitutions $T=V_jV_{\eta,\lambda}$ of distinct invariants $\alpha/\gamma=\lambda\tau/\tau=\lambda$. We choose these as the $q^k=fq^k$ extenders V_j and set $\alpha_j/\gamma_j=\lambda_j$. We find as in 4° [Case $A_{q=2}^{k\geq 1}$] that $\beta_j/\gamma_j=\lambda'$ and $\gamma_j^2=\lambda_j''=\kappa_j$; whence $\gamma_j=\eta_j$. Thus V_j has the form

$$V_j=(\lambda_j\eta_j,\ \lambda_j'\eta_j;\ \eta_j,\ \lambda_j'''\eta_j)\ . \tag{16}$$

V_j or $V_jV_{\eta_0,0}$ has the form (13) according as η_j is an even or an odd power of $\eta_0=\sqrt{\kappa_0}$; we denote it by V_j'.

When we extend the $G^{(\infty)}_{\frac{1}{2}q^k(q^k-1)}\{V_{\kappa,\lambda}\}$ by these q^k V_j' we obtain the $G_{M(q^k)}$ of the caption theorem. Since $P_{\eta_0}^2=P_{\eta_0^2}=P_{\kappa_0}$ and $P_{\eta_0}\,G_{M(q^k)}\,P_{\eta_0}^{-1}=G_{M(q^k)}$, this group $G_{M(q^k)}$ extends by $P_{\eta_0}=V_{\eta_0,0}$ to the $G_{2M(q^k)}$ of the caption theorem which is therefore our group G_Ω of order $\Omega=2M(q^k)$.

[Case $B_{f=3}$] *Theorem: The group $G_{\Omega=60}$ is a subgroup of the group $G_{M(3^2)}=G_{360}$ of the type A (8) depending on the $GF[3^2]$. It is generated by the generators*

$$E_1=S_{-1}=\left(\frac{1,-1}{0,1}\right)\ ,\quad E_2=T_{0,\sqrt{-1}}=\left(\frac{\sqrt{-1},0}{1,-\sqrt{-1}}\right)\ ,\quad E_3=P_{\sqrt{-1}}=\left(\frac{\sqrt{-1},0}{0,-\sqrt{-1}}\right) \tag{17}$$

subject to the generational relations

$$I=E_1^6=E_2^2=E_3^2=(E_1E_2)^3=(E_1E_3)^2=(E_2E_3)^5\ , \tag{18}$$

and hence (§ 1) *is an icosahedron group.*

We have $q=3$, $k=1$, $n=$ even, $\Omega=60$, $f=3$. The $q^k-1=2$ marks κ are $\kappa=+1,-1$; the marks λ are $\lambda=0,+1,-1$; the marks η are $\eta=+1,-1$, $+\sqrt{-1},-\sqrt{-1}$. $\kappa_0=-1$; $\eta_0=\sqrt{-1}$.

The G_Ω contains the group $G^{(\infty)}_{q^k(q^k-1)}=G_6^{(\infty)}\{V_{\eta,\lambda}\}$, which is obtained by extending the $G_3^{(\infty)}\{V_{\kappa,\lambda}=S_\lambda\}$ by $T_0=P_{\eta_0}(9)$, and also the substitution T_0' (11). In T_0' τ is not a mark η; if it were, the $G_{\Omega=60}$ would contain (§ 7) a subgroup $G_{2M(3)}=G_{24}$ (13).

The $G_6^{(\infty)}\{V_{\eta,\lambda}\}$ extends to the $G_{\Omega=60}$ by the identity and certain nine extenders V_j; since in (12) the equality holds we may take every extender as a substitution $T=T_j$ of period 2; then the three extenders $T_j=T_j'=T_\lambda'$ (15) ($j=1,2,3$; $\lambda=1,-1,0$) with invariants $\lambda=1,-1,0$ yield each two substitutions $T=T_jV_{\eta,\lambda}$, while the remaining six extenders T_j ($j=4,\cdots,9$) yield each one substitution $T=T_jV_{\eta,\lambda}$.

Analyzing the $G_{\Omega=60}$ with respect to its 18 substitutions $V_jV_{\eta,\lambda}$ of set I (3°), and remembering that an extender V_j yields at most $2d_-=4$ such substitutions $V_jV_{\eta,\lambda}$ (3°), we find in our G_Ω that (1) no extender $V_j=T_j$ yields 4, (2) the three extenders

T'_λ yield 0, and hence (3) the remaining six extenders T_j yield each 3 such substitutions of set I, and then (4) these six T_j are exactly the six $T = T_{\lambda,\eta'}$, with $(\alpha, \beta, \gamma, \delta) = (\lambda + \eta', \beta, 1, -\lambda - \eta')$ where $\alpha\delta - \beta\gamma = 1$ for $\lambda = 0, +1, -1$; $\eta' = \eta_0, -\eta_0$.

The $G_{\Omega=60}$ is then, if indeed it exist at all, determined uniquely by the $G_6^{(\infty)}\{V_{\eta,\lambda}\}$ and the six extenders $T_{\lambda,\eta'}$ as a subgroup of the $G_{M(3^n)=360}$ of type A (8) depending upon the $GF[3^2]$; this group is a subgroup of the fundamental $G_{M(3^n)}$, since n is even.

Now the three substitutions (17) which satisfy the relations (18) generate (by § 1) an icosahedron group G_{60}. This actually existing icosahedron subgroup G_{60} of the $G_{M(3^n)}$ (n = even) is easily seen to be the (hypothetical) $G_{\Omega=60}$ of our present analysis [Case $B, f = 3$].

(6°) *The systems of conjugate groups determined by the various* $G_\Omega(2°, \cdots, 5°)$.

We have $(2°, \cdots, 5°)$ separated the subgroups G_Ω of the $G_{M(s)}$ of linear fractional substitutions of determinant 1 in the $GF[s = q^n]$ (§ 4) which contain substitutions of period q and are subgroups of no one of the $s + 1$ $G^{(\mu)}_{\frac{s(s-1)}{2;1}}$ into four classes I $\cdots$ IV. The subgroups $G_{\Omega\,\mathrm{I}} \cdots G_{\Omega\,\mathrm{IV}}$ of these respective classes are under the $G_{(2;1)M(s)}$ of all substitutions in the $GF[s]$ (§ 4) conjugate with

(I) [A] a $G_{\mathrm{I}(k)} = G_{M(q^k)}$ (8), where k is a divisor of n;

(II) $[\mathrm{B}_{f=1,\,q>2,\,n/k=\text{even}}]$ a $G_{\mathrm{II}(k)} = {}_2G_{M(q^k)}$ (13), where k is a divisor of n with even n/k;

(III) $[\mathrm{A}_{q^k=2^1}]$ a dihedron $G_{\mathrm{III}(f)} = G_{2(1+2f)}$, where $1 + 2f$ is a divisor of $q^n - 1 = 2^n - 1$;

(IV) $[\mathrm{B}_{f=3,\,q=3,\,k=1,\,n=\text{even}}]$ the G_{IV} = the icosahedron G_{60} (17).

These typical groups $G_{\mathrm{I}(k)}$ $G_{\mathrm{II}(k)}$ $G_{\mathrm{III}(f)}$ G_{IV} actually exist under the conditions just now specified.

The $G_{\mathrm{I}(k)} = G_{M(q^k)}$ is simple (§ 8).

The $G_{\mathrm{II}(k)} = G_{2M(q^k)}$ contains $G_{M(q^k)} = G_{\mathrm{I}(k)}$ as the only proper self-conjugate subgroup for $q^k > 3$; the $G_{2M(3^1)}$ is an octahedron group G_{24} (§ 1), and contains the self-conjugate $G_{M(3^1)}$ and also a self-conjugate four-group.

The $G_{\mathrm{III}(f)} = G_{2(1+2f)}$ contains as its self-conjugate subgroups the cyclic subgroups of its cyclic base G_{1+2f}.

The $G_{\mathrm{IV}} = G_{60}$ is simple.

Within the $G_{M(s)}$ any such group G_Ω is self-conjugate under a $G_{\Omega'}$, which is likewise a group G_Ω. The two groups $G_\Omega, G_{\Omega'}$ may be simultaneously transformed each to its typical form (I $\cdots$ IV).

Within the $G_{M(s)}$ each group $G_{\Omega\mathrm{II}}$, $G_{\Omega\mathrm{III}}$, $G_{\Omega\mathrm{IV}}$ is self-conjugate under itself and so is one of a system of $M(s)/\Omega$ conjugate groups.

Since the $G_{\mathrm{I}(k)}$ is self-conjugate under the $G_{\mathrm{II}(k)}$, $G_{\mathrm{I}(k)}$; $G_{\mathrm{I}(k)}$ according as $(q > 2)$ n/k = even, n/k = odd; $(q = 2)$, each group $G_{\Omega\mathrm{I}(k)}$ is one of a system of $M(s)/(2, 1; 1)\Omega$ conjugate groups.

The question remains as to the number of such conjugate systems in the various cases, for we have (2°) introduced a reducing transformer $P_{\sqrt{\lambda_0^{-1}}}$ which is in the $G_{(2;1)M(s)}$, and in the $G_{M(s)}$ only if the mark λ_0 is a square in the $GF[q^n]$. There is then only one such system of conjugate groups G_Ω if $q=2$ ($G_{\Omega I}$, $G_{\Omega III}$) (since then every mark λ_0 ($\lambda_0 \neq 0$) is a square) or if $q>2$, $n/k=$ odd ($G_{\Omega I}$) (since then every $[\lambda_1, \cdots, \lambda_{m=k}]$ with the $GF[q^k]$ as multiplier field has besides the mark 0 half its marks squares and half not-squares, and since we may choose for λ_0 any one of its square marks). But there are two such systems of conjugate groups G_Ω ($G_{\Omega I}$, $G_{\Omega II}$, $G_{\Omega IV}$) if $q>2$, $n/k=$ even, which interchange under the transformer $P_{\sqrt{\nu}}=D_\nu$ where ν is any not-square in the $GF[q^n]$.

The results for $q>2$ just stated may well be obtained otherwise by consideration within the $G^{s^2+1}_{M(s^2=q^{2n})}$, of which the $G^{s^2+1}_{M(s)}$ and the $G^{s^2+1}_{2M(s)}$ are subgroups. If $q>2$, $n/k=$ even, then each group $G_{\Omega I(k)}$, $G_{\Omega II(k)}$, $G_{\Omega IV}$ is within the $G_{M(q^n)}$ or within the $G_{M(q^{2n})}$ self-conjugate under the same group; hence every system of conjugate groups under the $G_{2M(s)}$ breaks into two systems of conjugate groups under the $G_{M(s)}$. But if $q>2$, $n/k=$ odd, and so $q>2$, $2n/k=$ even, then each group $G_{\Omega I(k)}=G_{M(q^k)}$ is within the $G_{M(q^n)}$ self-conjugate under itself but in the $G_{M(q^{2n})}$ self-conjugate under a $G_{2M(q^k)}=G_{\Omega II(k)}$; hence every system of conjugate groups under the $G_{2M(s)}$ remains a system of conjugate groups under the $G_{M(s)}$.

(7°) *The subgroups* $G_\Omega(2° \cdots 5°)$ *of the* $G_{2M(s)}$ ($q>2$) *and their systems of conjugate groups.*

We find that the $G_{2M(s)}$ contains the representative groups

(I) $[A]$ a $G_{I(k)}=G_{M(q^k)}$ (8), where k is a divisor of n;

(II) $[B_{f=1,q>2}]$ a $G_{II(k)}=G_{2M(q^k)}$ (13), where k is a divisor of n;

(IV) $[B_{f=2,q=2,k=1,n=\text{even}}]$ the $G_{IV}=G_{60}$ (17),

whose systems contain respectively (I) $2M(s)/2\Omega I(k)$; (II) $2M(s)/\Omega II(k)$; (IV) $2M(s)/\Omega IV$ groups, every $G_{I(k)}$ being self-conjugate under a corresponding $G_{II(k)}$.

(8°) *The tetrahedron and the octahedron subgroups* G_Ω *of the* $G_{M(s)}$.

The only typical subgroups G_Ω (I $\cdots$ IV) of order 12 and 24 are (I) the $G_{M(3^1)=12}$ of the $G_{M(3^n)}$ and (II) the $G_{2M(3^1)=24}$ of the $G_{M(3^n)}$ ($n=$ even). These are respectively a tetrahedron and an octahedron group (§ 1). Each contains a single self-conjugate four-group. The groups G_{12}; G_{24} of these types are for $n=$ odd; even the largest groups containing four-groups as self-conjugate subgroups (§ 9 end). The statements (of 6°) as to systems of conjugate groups G_{12}, G_{24} for $q=3$ are given below (§ 15, 1°).

(9°) *The icosahedron subgroups* G_Ω *of the* $G_{M(s)}$.

The only typical subgroups G_Ω (I $\cdots$ IV) of order 60 are (I) the $G_{M(5)=60}$ of the $G_{M(5^n)}$, (I) the $G_{M(2^2)=60}$ of the $G_{M(2^n)}$ ($n=$ even), and (IV) the G_{IV} of the $G_{M(3^n)}$ ($n=$ even). Each of these is an icosahedron group (§ 1). The statements (of 6°) as to systems of conjugate groups G_{60} are given below (§ 16, 3°).

§14. SUBGROUPS OF $G_{M(q)}$ CONTAINING NO OPERATORS OF PERIOD q

(1°) *The diophantine equations.*[28]

The G_Ω contains only substitutions of sets II and III (§ 6). Every substitution of G_Ω lies in and determines within G_Ω a largest cyclic subgroup G_d. Two such groups G_d have only the identity in common. Every G_d is within G_Ω one of a system of Ω/fd conjugate groups, where f is either 1 or 2, according as the G_d is self-conjugate within itself or within a dihedron G_{2d} based on itself.

The G_Ω contains say r such systems. Then the enumeration of the Ω substitutions of G_Ω leads to the relations

$$\Omega = 1 + \sum_{i=1}^{r} (d_i - 1)\,\Omega/f_i d_i \qquad (f_i = 1 \text{ or } 2)\,, \tag{1}$$

$$\Omega \geqq f_i d_i \qquad (i = 1, 2, \ldots, r)\,. \tag{2}$$

Further, if two non-conjugate cyclic groups G_{d_i}, G_{d_j} of *odd* order are present, then there are at least d_j groups in the system determined by G_{d_i}, and *vice versa*, so that

$$\Omega \geqq 2\,d_i d_j - d_i - d_j + 1\,. \tag{3}$$

The discussion of the relations (1, 2, 3) leads to the six cases:

Case	r	d_1 d_2 d_3	f_1 f_2 f_3	Ω
I	1	d	1	d
II	2	d 2	2 1	$2d$
III	3	d 2 2	2 2 2	$2d$
IV	2	3 2	1 2	12
V	3	4 3 2	2 2 2	24
VI	3	5 3 2	2 2 2	60

(2°) We discuss these cases more narrowly from our present group-theoretic standpoint.

[Case I.] The $G_{\Omega=d}$ is a cyclic G_d of § 9.

[Case II.] The $G_{\Omega=2d}$ is a dihedron G_{2d} with d odd of § 9.

[Case III.] The $G_{\Omega=2d}$ is a dihedron G_{2d} with d even of § 9.

[Case IV.] This case occurs only for $q \neq 2, 3$. The $G_{\Omega=12}$ contains a system of four groups G_3, each self-conjugate exactly under itself. These contain only the identity in common. Accordingly the G_{12} is holoedrically isomorphic with a substitution-group G_{12}^4 of order 12 on 4 letters. This G_{12}^4 is the alternating $G_{4!1}$, and so *the G_{12} is a tetrahedron group.* It contains one self-conjugate four-group G_4—the dihedron G_4 in which each of the three conjugate $G_{d_2=2}$ is self-conjugate.

[Case V.] This case occurs only for $q \neq 2, 3$. The $G_{\Omega=24}$ contains a system of four cyclic groups G_3 and correspondingly a system of four dihedron groups G_6. These

[28] The equation (1) originated in C. JORDAN'S analytic attack (*Crelle*, Vol. LXXXIV, 1878) on the problem of the determination of all finite groups of binary and ternary linear substitutions. *Cf.* GIERSTER, *loc. cit.*, pp. 358 f., and KLEIN-FRICKE, *loc. cit.*, pp. 483 f.

G_4 contain only the identity in common.[29] Accordingly the G_{24} is holoedrically isomorphic with a substitution-group G_{24}^4 of order 24 on 4 letters. This G_{24}^4 is the symmetric group G_{41}^4, and so *the G_{24} is an octahedron group.* It contains one self-conjugate tetrahedron group G_{12} and one self-conjugate four-group G_4. (This G_4 contains the identity, and the three substitutions $V_4'^2$, $V_4''^2$, $V_4'''^2$ of period two, where V_4', V_4'', V_4''' are generators of the three conjugate cyclic G_4. For $V_4'^2$, $V_4''^2$, $V_4'''^2$ form a system of conjugate substitutions under the G_{24}; and they are commutative, since V_4' transforms $G_4\{V_4''\}$ into $G_4\{V_4'''\}$ and so $V_4'^2$ transforms $G_4\{V_4''\}$ into itself and hence $V_4''^2$ into itself.)

[Case VI.] This case occurs only for $q \neq 2, 3, 5$. The $G_{\Omega=60}$ contains a system of 15 conjugate substitutions of period 2. Each is self-conjugate in a four-group G_4. There are 5 such four-groups; they are conjugate under the G_{60}. Each G_4 is self-conjugate in a G_{12} of tetrahedron[30]-type (Case IV). There are five conjugate G_{12}, since each contains only one four-group. These G_{12} have only the identity in common. Hence the G_{60} is holoedrically isomorphic with a substitution-group G_{60}^5 of order 60 on 5 letters. This G_{60}^5 is the alternating $G_{15!}^5$, and so *the G_{60} is an icosahedron group.*

§ 15. THE TETRAHEDRON AND THE OCTAHEDRON SUBGROUPS OF THE $G_{M(s)}$

(1°) From § 13 (8°) and § 14 (Cases III and IV) and the four-group considerations of § 9 and for $q = 2$ from § 12 (2°) we see easily:

[$s = q^n = 8h \pm 1$.] *The $G_{M(s)}$ contains two systems of $M(s)/24$ conjugate octahedron groups G_{24} and two systems of $M(s)/24$ conjugate tetrahedron groups G_{12}. Every G_{12} is self-conjugate under a G_{24}. The two systems coalesce into one system within the $G_{2M(s)}$. The $G_{2M(s)}$ contains no other tetrahedron or octahedron groups.*

[$s = q^n = 8h \pm 3$] and [$s = 2^n$ (n even).] *The $G_{M(s)}$ contains no octahedron group G_{24} and one system of $M(s)/12$ conjugate tetrahedron groups G_{12}. For $q > 2$ the $G_{2M(s)}$ contains one system of $M(s)/12$ conjugate octahedron groups G_{24} containing respectively these G_{12}. The $G_{2M(s)}$ contains no other tetrahedron or octahedron groups.*

For $q > 2$ the $G_{2M(s)}$ always contains tetrahedron G_{12} and octahedron G_{24}, and the $G_{M(s)}$ always contains the G_{12}, and, when 24 is a divisor of $M(s)$, also the G_{24}.

For $q = 2$, although the order $M(2^n)$ is a multiple of 12 for $n > 1$ and of 24 for $n > 2$, the group $G_{M(2^n)}$ contains tetrahedron G_{12} only for n even, and octahedron G_{24} never.

(2°) We exhibit generators of representatives of these systems of groups conjugate within the $G_{(2;1)M(s)}$.

[$s = 2^n$, n even] $G_{12}\{E_1, E_2\}$ *of the* $G_{M(2^n)}^{2^n+1}$:

$$E_1 = (\kappa, 0; 0, \kappa^{-1}), \quad E_2 = (1, 1; 0, 1) \qquad (\kappa^2+\kappa+1=0).$$

[29] The four G_2 contain only the identity in common. The four G_4 do not contain two substitutions of period 2 in common, since then the four G_4 and so the four G_2 would be identical. The four G_4 do not contain in common one single substitution of period 2, since this substitution would be self-conjugate in the G_{24} and this G_{24} contains no self-conjugate substitution.

[30] Since no G_{12} of either of cases VI, V, III, II, I contains a self-conjugate four-group.

[$q > 2$] $G_{12}\{E_1, E_2\}$, $G_{24}\{B_0, B_1, B_2\}$ *of the* $G^{s+1}_{2M(s)}$ *or of the* $G^{\prime s^2+1}_{2M(s)}$, *according as* $s = q^n = 4k+1$ *or* $4k-1$:

$$E_1 = \begin{pmatrix} \frac{1+\sqrt{-1}}{2} & \frac{-(1+\sqrt{-1})}{2} \\ \frac{1-\sqrt{-1}}{2} & \frac{1-\sqrt{-1}}{2} \end{pmatrix}, \quad E_2 = \begin{pmatrix} 0, -1 \\ 1, 0 \end{pmatrix}.$$

$$B_0 = (1, 1; 1, -1) = (\sqrt{\rho}, \sqrt{\rho}; \sqrt{\rho}, -\sqrt{\rho}), \quad B_1 = B_0 E_1, \quad B_2 = B_0 E_2.$$

The case $q = 2$ is given in § 12, 3°.

The case $q > 2$ is treated thus: Attending to the properties of the abstract tetrahedron and octahedron groups (§ 1) and starting from the representative four-group (§ 9) of the $G_{M(s)}$—in suitable form—

I, $K = (\sqrt{-1}, 0; 0, -\sqrt{-1})$, $L = (0, -1; 1, 0)$, $M = KL = (0, \sqrt{-1}; \sqrt{-1}, 0)$, we set down for an operator U of the $G_{M(s)}$ the system of equations

$$U^2 = I, \quad UK = LU, \quad UL = MU, \quad UM = KU,$$

and find the four solutions

$$U = U_{e_1, e_2} = \begin{pmatrix} \frac{1+e_1\sqrt{-1}}{2} & \frac{-e_2(1+e_1\sqrt{-1})}{2} \\ \frac{e_2(1-e_1\sqrt{-1})}{2} & \frac{1-e_1\sqrt{-1}}{2} \end{pmatrix} \qquad (e_1 = \pm 1, e_2 = \pm 1),$$

which all belong to the tetrahedron group

$$G_{12}\{E_1, E_2\} : \quad E_1 = U_{1,1}, \quad E_2 = L : \quad I = E_1^3 = E_2^2 = (E_1 E_2)^3.$$

Then the substitution B_0 of the $G_{2M(s)}$ uniquely determined by the equations

$$I = B_0^2 = (B_0 E_1)^3 = (B_0 E_2)^2$$

extends the $G_{12}\{E_0, E_1\}$ to the octahedron group

$$G_{24}\{B_0, B_1, B_2\} : I = B_0^2 = B_1^2 = B_2^2 = (B_0 B_1)^3 = (B_0 B_2)^3 = (B_1 B_2)^3.$$

The $G_{24}\{B_0, B_1, B_2\}$ does or does not belong to the $G_{M(s)}$ according as $-1, -2$ are or are not of the same quadratic character (square or not-square) in the $GF[q^n]$. The supplementary quadratic reciprocity theorem

$$\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}$$

exhibits the accord of this statement with that of (1°).

In case within the $G_{M(s)}$ there are *two* systems of conjugate groups a representative of the second system is obtained from a representative of the first by transforming say by D_ρ.

§ 16. THE ICOSAHEDRON SUBGROUPS OF THE $G_{M(s)}$

(1°) We seek within the $G_{M(s)}$ a system of three generators E_1, E_2, E_3 of an icosahedron group G_{60} which satisfy the generational relations of § 1

$$I = E_1^2 = E_2^2 = E_3^2 = (E_1 E_2)^3 = (E_1 E_3)^3 = (E_2 E_3)^3. \qquad (1)$$

The treatment is such as not to include the case $q = 3$. The icosahedron groups of the $G_{M(q=3^n)}$ have however been determined in § 13, 9°.

The generators E_1, E_2 determine a dihedron group G_2. Under the $G_{(2;1)M(q)}$ ($q \neq 3$) they are (§§ 9, 6) respectively simultaneously conjugate with

$$E_1 = \left(\frac{E,\ 0}{0,\ E^{-1} = -E-1}\right), \quad E_2 = T = \left(\frac{0,\ -1}{1,\ 0}\right), \tag{2}$$

where we are working in the real $G^{s+1}_{M(q)}$ or in the second imaginary $G'^{s^2+1}_{M(q)}$ (§ 5) according as $\frac{s-1}{2;\,1}$ or $\frac{s+1}{2;\,1}$ is divisible by 3, or, what must be the same thing,[31] according as the mark E, ($E \neq 1$ since $q \neq 3$), satisfying the equations

$$E^3 = 1, \quad E^2 + E + 1 = 0, \quad (2E+1)^2 = -3, \tag{3}$$

does or does not belong to the $GF[q^n]$, *i. e.*, according as -3 is a square or not-square in the $GF[q^n]$, if $q > 3$, and according as n is even or odd, if $q = 2$.

We seek then a substitution

$$E_2 = (A, B;\ C, -A) \qquad (-AA-BC=1) \tag{4}$$

of period 2 such that the products

$$E_1E_2 = \left(\frac{EA,\ EB}{-(E+1)C,\ (E+1)A}\right), \quad E_2E_3 = \left(\frac{B,\ -A}{-A,\ -C}\right) \tag{5}$$

shall be each of period 3, and so under the $G_{M(q)}$ conjugate (§ 6 II, III) with E_1. The necessary and sufficient conditions (§ 6, IV) are

$$A^2 + BC = -1, \quad (1+2E)A = 1, \quad B - C = \pm 1, \tag{6}$$

where the second equation implies that in (4) the proper normalization of E_2 is chosen (§ 4 (7)).

[Case $q = 2$.] We find at once two solutions E_2, viz.:

$$E_2' = (1, 1;\ 0, 1) \quad E_2'' = (1, 0;\ 1, 1), \tag{7}$$

and so have two icosahedron groups $G_{60}\{E_1, E_2', E_3\}$ and $G_{60}\{E_1, E_2'', E_3\}$. Since the E_2', E_2'' have neither imaginary form (§ 5 (17, 18)), the groups must be subgroups of the real $G_{M(q)}$ (if of any $G_{M(q)}$); they are subgroups of the real $G_{M(q)}$ if and only if n is even; in that case E_1 is real; indeed the mark E (3) defines the $GF[2^2]$ and we determine by either set of three generators the (same) icosahedron $G_{60} = G_{M(2^2)}$ of § 13, 8°.

[Case $q > 3$.] We find easily

$$A = -\tfrac{1}{3}(2E+1), \quad B = \tfrac{1}{2}(F \pm 1), \quad C = \tfrac{1}{2}(F \mp 1), \quad A^2 = -\tfrac{1}{3}, \quad F^2 = -\tfrac{5}{3}, \tag{8}$$

and have in all four or two sets of generators $\{E_1, E_2, E_3\}$ according as $q > 5$ or $q = 5$. It is easy to show that these groups $G_{60}\{E_1, E_2, E_3\}$ are (all) subgroups of the

[31] This (for $q > 3$) is a proof of the reciprocity-formula $\left(\frac{-3}{q}\right) = \left(\frac{q}{3}\right)$.

$G_{M(s)}$ in its real or second imaginary form (§5 (17, 18)) if and only if 5 is a square or 0 in the $GF[q^n]$, that is, in case n is even for every prime q, and in case n is odd for primes q of the form $q = 5$ or $5k+1$ or $5k-1$. (We have used the quadratic reciprocity theorem.)

It is important to observe that the $G_{M(s)}$ contains an icosahedron G_{60} whenever it contains an operator of period 5, that is, if s has the form 5^n or $5k+1$ or $5k-1$. (The cases $q=3$, $n=$ even, and $q=2$, $n=$ even are included.)

In the $G_{M(s)}$ $(q>3)$ there are (§9) $M(s)/6$ dihedron groups G_6 and for each 2.3 generations $\{E_1, E_3\}$. In the $G_{M(s)}$ there are $M(s)$ dihedron sets $\{E_1, E_3\}$ and, if any, 4 $M(s)$ or 2 $M(s)$ icosahedron sets $\{E_1, E_2, E_3\}$ according as $q>5$ or $q=5$.

In particular, the icosahedron $G_{M(5)=60}$ has 60 sets $\{E_1, E_3\}$ and for each such set 2 sets $\{E_1, E_2, E_3\}$. The 60 sets $\{E_1, E_3\}$ are conjugate under the $G_{M(5)}$ (§9). The 120 sets $\{E_1, E_2, E_3\}$ fall into two systems each of 60 sets conjugate under the $G_{M(5)}$. Of these two systems the two sets $\{E_1, E_2', E_3\}$, $\{E_1, E_2'', E_3\}$

$$E_1=\left(\frac{E,\ 0}{0,\ E^{-1}=-E-1}\right),\quad E_2'=\left(\frac{E+3,\ \pm 3}{\mp 3,\ -E-3}\right),\quad E_3=\left(\frac{0,\ -1}{1,\ 0}\right) \tag{9}$$

are representatives. We notice the relation

$$\left(\frac{0,\ -1}{1,\ 0}\right)\left(\frac{A,\ B}{C,\ D}\right)\left(\frac{0,\ 1}{-1,\ 0}\right)=\left(\frac{-D,\ C}{B,\ -A}\right). \tag{10}$$

Hence

$$E_3E_2''E_3^{-1}=E_2'. \tag{11}$$

Similar relations hold for the abstract and so for every concrete icosahedron group.

In particular: For $q=5$, $n=$ any, the two sets $\{E_1, E_2, E_3\}$ (2, 3, 4, 8) yield the same icosahedron group. For $q>5$, the four sets $\{E_1, E_2, E_3\}$ yield two groups G_{60} differing only in the choice of F as root of $F^2=-5/3$. These two groups[32] are conjugate within the $G_{2M(s)}$ by the transformer D_{-1} $(\omega'=-\omega)$.

Hence, *the* $G_{M(s)}$ $(s=q^n=5^n$ or $5k\pm1$, $q>3)$ *contains* $M(s)/30$ $(q>5)$, *or* $M(s)/60$ $(q=5)$ *icosahedron groups* G_{60}, *all within the* $G_{2M(s)}$ *conjugate with the group* G_{60} $\{E_1, E_2, E_3\}$,

$$E_1=\left(\frac{E,\ 0}{0,\ E^{-1}=-E-1}\right),\quad E_2=\left(\frac{-\frac{1}{3}(2E+1),\ \frac{1}{3}(F+1)}{\frac{1}{3}(F-1),\ \frac{1}{3}(2E+1)}\right),\quad E_3=\left(\frac{0,\ -1}{1,\ 0}\right), \tag{12}$$

where E *and* F *are* (*any*) *particular roots of the respective equations.*

$$E^2+E+1=0,\quad 3F^2+5=0. \tag{13}$$

[32] Since within an icosahedron group G_{60} the 60 dihedron sets $\{E_1, E_3\}$ are conjugate, if the dihedron sets $\{E_1, E_2\}$ of the $G_{M(s)}$ fall into two systems of conjugate sets (*i. e.*, if $(s\mp1)/6$ is even (§9), *i. e.*, if $s=12h+1$ or $12h+11$), then the icosahedron groups G_{60} of the $G_{M(s)}$ must fall correspondingly into two systems, and the two groups $G_{60}\{E_1, E_2, E_3\}$ containing the same dihedron $G_{2.3}\{E_1, E_2\}$, must be conjugate *within the* $G_{M(s)}$ (and in fact, in this case D_{-1} belongs to the $G_{M(s)}$, in its real or second imaginary form, according as $s=12h+1$ or $12h+11$).

(2°) We inquire under what groups G_{60t} $(t \geqq 1)$ of the $G_{2M(s)}$ and of the $G_{M(s)}$ respectively this $G_{60}\{E_1, E_2, E_3\}$ (12) is self-conjugate. Since under the G_{60} itself the various system $\{E_1, E_3\}$ are conjugate, we seek a substitution U which transforms the system $\{E_1, E_3\}$ and the group $G_{60}\{E_1, E_2, E_3\}$ each into itself. $U = I$ and $U = D_{-1}$ are the only substitutions transforming $\{E_1, E_3\}$ into itself. $U = D_{-1}$ transforms $G_{60}\{E_1, E_2, E_3\}$ into itself, if and only if $q = 5$. Now for $q = 5$

$$U = D_{-1} = (-1, 0; 0, 1) = (-\sqrt{\rho}, 0; 0, \sqrt{\rho})$$

belongs to the $G_{2M(s)}$ in its real or its second imaginary form, and to the real $G_{M(s)}$, but not to the second imaginary $G_{M(s)}$. Hence for $q > 5$, the $G_{60}\{E_1, E_2, E_3\}$ is within the $G_{2M(s)}$ or the $G_{M(s)}$ self-conjugate exactly under itself, while, for $q = 5$, the $G_{60}\{E_1, E_2, E_3\}$ is within the $G_{2M(s)}$ self-conjugate under the $G_{120}\{E_1, E_2, E_3, D_{-1}\}$ of the type $G_{2M(5)}$ (§ 13, 5° B, 6° II; $q = 5$, $k = 1$), and within the $G_{M(s)=M(5^n)}$ under this G_{120} or under itself, according as n is even or odd, *i. e.*, according as -3 is or is not a square in the $GF[5^n]$.

(3°) Hence finally for all cases:

[Case $q = 5$.][33] *In the* $G_{M(s=5^n)}$ *there are* $M(s)/60$ *icosahedron groups* $G_{60} = G_{M(5)}$ *conjugate within the* $G_{2M(s)}$ *and forming within the* $G_{M(s)}$ *two systems or one system of conjugate groups according as n is even or odd.*

[Case $q \neq 5$.][34] *In the* $G_{M(s)}$ $(s = q^n = 5k \pm 1)$ *there are* $M(s)/(30; 60)$ *icosahedron groups* G_{60} *conjugate within the* $G_{(2;1)M(s)}$ *and forming within the* $G_{M(s)}$ $(2; 1)$ *systems of* $M(s)/60$ *conjugate groups.*

Of course, whenever within the $G_{M(s)}$ $(q > 2)$ there are two systems, one obtains the representative of the second system by transforming by D_ρ the representative of the first system, viz., of the (one) system within the $G_{2M(s)}$.

§ 17. THE ABSTRACT GROUP $G_{M(s)}$ IS HOLOEDRICALLY ISOMORPHIC TO THE (DOUBLY TRANSITIVE) SUBSTITUTION-GROUP $G^{s+1}_{M(s)}$ OF DEGREE $s+1$ AND TO A GROUP $G^D_{M(s)}$ OF LOWER DEGREE D $(D < s+1)$ ONLY[35] IN THE CASES $s = q^n = 5, 7, 11, 3^2$; $M(s) = 60, 168, 660, 360$; $D = 5, 7, 11, 6$ (WHEN THE $G^D_{M(s)}$ IS RESPECTIVELY 3-, 2-, 2-, 4-PLY TRANSITIVE).

For $n = 1$, *the theorem of the caption is a celebrated theorem due to Galois and Gierster.*

(1°) For $s = 2, 3$ the theorem is evident.

The $G_{M(s)}$ $(s \neq 2, 3)$ is simple (§ 8). A substitution-group $G^D_{M(s)}$ is simple, only if it is (holoedrically isomorphic, or, say, for brevity) equivalent to its transitive constituents. We consider then, first, the *transitive* $G^D_{M(s)}$ equivalent to our $G_{M(s)}$. This equivalence implies the existence in the $G_{M(s)}$ of a (complete) system of D conjugate groups G_Ω $(D\Omega = M(s))$ (which have no common subgroup—and they do not, since

[33] *Cf.* § 13, 9°. [34] *Cf.* § 13, 9° for $q = 2, 3$. I communicated to Mr. Fricke in a letter dated February 17, 1894.

[35] This theorem (apart from the parenthetical remarks)

the $G_{M(s)}$ is simple), and, conversely, if the $G_{M(s)}$ contains such a system of D groups G_Ω, then the operators of the $G_{M(s)}$ *qua* transformers of these groups determine a $G^D_{M(s)}$ equivalent to our $G_{M(s)}$.

We find that the $s+1$ conjugate groups $G^{(\kappa)}_{\frac{s(s-1)}{2};1} = \frac{M((s)}{(s+1)}$ (§ 12) of the $G_{M(s)}$ ($s \neq 2, 3$), which lead to the equivalent doubly transitive $G^{s+1}_{M(s)}$, have higher order than any other groups G_Ω of the $G_{M(s)}$, for $s > 11$. Of the groups $G_{M(s)}$ ($s \leqq 11$, $s \neq 2, 3$) subgroups of respectively (equal or, in fact), higher order occur in the cases $s = 5, 7, 11, 3^2$, viz., respectively, the one system of 5 G_{12} (§ 15), the two systems of 7 G_{24} (§ 15), the two systems of 11 G_{60} (§ 16), the two systems of 6 G_{60} (§ 16). Thus we have the $G^5_{M(5)}$, the $G^7_{M(7)}$, the $G^{11}_{M(11)}$, the $G^6_{M(3^2)}$ of the caption theorem — for the *two* $G^7_{M(7)}$ are similar, since under transformation by D_ρ the $G_{M(s)}$ is invariant and the two systems of conjugate groups interchange, and similarly for the two $G^{11}_{M(11)}$ and for the two $G^6_{M(3^2)}$.

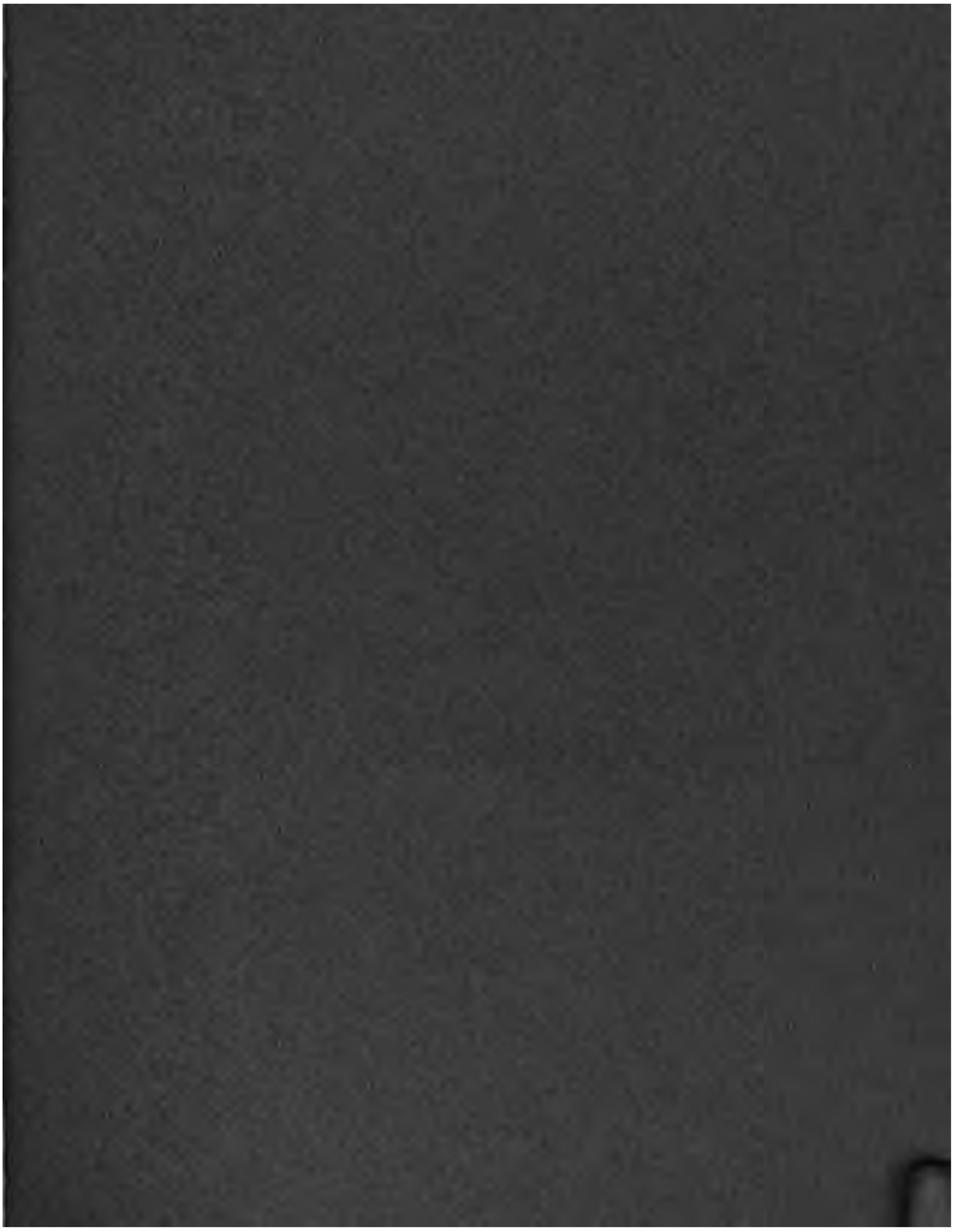
The degree of an *intransitive* $G^D_{M(s)}$ equivalent to the $G_{M(s)}$ is the sum of the respective degrees of its two or more transitive constituents. It is clear that every such intransitive $G^D_{M(s)}$ is of degree $D > s+1$.

(2°) The $G^5_{M(5)=60}$ and the $G^6_{M(3^2)=360}$ are of course respectively the triply, quadruply transitive alternating groups $G^5_{\mathfrak{A}5!}$, $G^6_{\mathfrak{A}6!}$ (*cf.* also § 1, 5°).

The $G^7_{M(7)=168}$ is doubly transitive.—For in the $G_{M(7)}$ the 7 conjugate octahedron groups G'_{24} (of either system) are the elements of a triple system Δ'_7.—For the $G_{M(7)}$ has two systems of 7 G_{24} (§ 15) $-G'_{24}$, $G''_{24}-$ and two systems of 7 four-groups $G_{2.2}$ (§ 9) $-G'_{2.2}$, $G''_{2.2}$. An octahedron G_{24}, *e. g.*, the $G_{2\,M(3)}$ (§ 1, 5°), contains a self-conjugate four-group $G'_{2.2}$ and a system of 3 conjugate four-groups $G''_{2.2}$ (§ 9). Every G'_{24} contains 3 $G''_{2.2}$ conjugate in itself and so in the $G_{M(7)}-$ say 3 $G'_{2.2}$. And every $G'_{2.2}$ lies in 3 G'_{24}. The 7 $G'_{2.2}$ determine then 7 triples of G'_{24}, in fact[36] a triple system Δ'_7.— Now all triple systems Δ_7 are similar. A Δ_7 has a (largest) group G^7_{168} (Δ_7) of order 168 and doubly transitive. Our $G^7_{M(7)}$ on the 7 G'_{24} is then *the* group G^7_{168} (Δ'_7) leaving invariant the triple system Δ'_7 in the 7 G'_{24}.

The $G''_{M(11)=660}$ is doubly transitive. — For the $G_{M(11)}$ contains two systems of 55 dihedron $G_{2.2}$ and two systems of 11 icosahedron G_{60} (§§ 9, 16); every G_{60} contains 10 conjugate $G_{2.2}$; every $G_{2.2}$ lies in two conjugate G_{60} (§ 16, 1°, footnote). Hence the $G_{M(11)}$ is transitive on the 11 G'_{60}; a G'_{60} is transitive on its 10 $G'_{2.2}$ and so on the remaining 10 G'_{60}. Thus the $G_{M(11)}$ is doubly transitive on the 11 G'_{60}. (Its order precludes its being triply transitive.)

[36] In the $G_{2\,M(3)}$ the three $G''_{2.2}$ contain each a (different) substitution V'_2 of the $G'_{2.2}$ (§ 9). A $G''_{2.2}$ and the $G'_{2.2}$ lie in and determine a dihedron $G_{2.4}$, containing two substitutions V''_2, three V_2, and two substitutions V'_4 of period 4, besides the identity. Two $G''_{2\,2}$ generate a group containing such a $G_{2.4}$ and another substitution V''_2 — and so the whole $G_{2\,M(3)=24}$. — Hence in the $G_{M(7)}$ two G'_{24} having a $G'_{2.2}$ in common do not have two $G_{2.2}$ in common. Thus no two triples of G'_{24} have two G'_{24} in common. The 7 triples contain then the 7.6 pairs of G'_{24} without duplication and without omission, and hence constitute a triple system Δ'_7.



BANS7 1965